CA Test Series

CA Final | Inter | Foundation Test Series

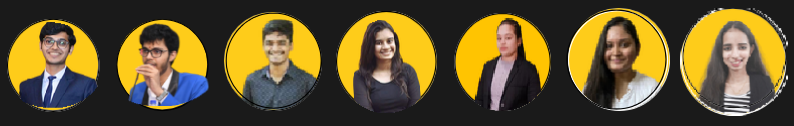
NOTE'S

CA INTER

EIS & SM

AMENDMENTS NOTES

Consistently Top AIRs from CA Test Series



EIS Amendments

Chapter 1

1. Risk Management - It is the "process of identifying risk, assessing risk, and taking steps to (prevent, if possible, or) reduce risk to an acceptable level and implementing the right mechanisms to maintain that level of risk". Risk management is a never-ending process. The risk management process comprises prevention and mitigation.

2. Risk analysis - Risk analysis is the activity in a risk management program where individual risks are identified. The first step in risk analysis is to appraise the value of an organization's assets. For example; If an asset has no value, then there is no need to provide protection for it. A primary goal of risk analysis is to ensure that only cost-effective safeguards are deployed.

3. Risk Management Strategies - Regardless of its overall risk appetite, when an organization identifies risks, the organization can take one of four possible actions:

1. Accept - The organization accepts the risk as is.

2.Mitigate/Treat (or reduce) - The organization acts to reduce the level of risk.

3. Transfer (or share) - The organization shares the risk with another entity, often an insurance company.

4. Avoid - The organization discontinues the activity associated with the risk.

All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks. The primary goal of risk management is to reduce risk to an acceptable level (i.e., residual risk). What is the level which is acceptable varies from one management to another, based on their risk appetite i.e. How much risk, they (management) are willing to accept rather than mitigate?

Chapter 3.

3. (Revised) The Functions of Information Systems - Information Systems have some basic functions, namely; inputs, processes, output and storage (IPOS). ISs collect (input) and

manipulate data (process), and generate and distribute reports (output) and based on the data-specific IT services, such as processing customer orders and generating payroll, are delivered to the organization. Finally, the ISS save (store) the data for future use. In addition to the four functions of IPOS, an information also needs feedback from its users and other stakeholders to help improve future systems. If alterations are needed to the system, adjustments are made by some form of control mechanism.

To enable efficient storage and retrieval of the content of databases organizations need to have a solid storage infrastructure. To ensure continuous business operations in case disaster strikes, organizations periodically back up their data to a secure location.

Q Environmental Controls

Fire damage

2. Controls for Environmental Exposures - M. IMP

1. Fire Alarms and Smoke Detectors Fire Alarms (both automatic and manual) should be purposefully placed - throughout the facility. In addition, Smoke-activated detectors are good for early warning devices. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station, for example, a fire station.

2. Fire Suppression Systems - Fire suppression systems are activated when extensive heat is generated due to fire. Fire suppression activities should start quickly, so that lives may be saved.

3. Fire Extinguishers - Hand-held Fire Extinguishers should be available in calculated locations throughout the area. The maintenance of fire extinguishers must be up to date.

4. Emergency Evacuation Plan - Employees should be taught the procedures for evacuation and damage control as well as how to use the fire protection equipment. Saving human lives is the first priority in any life-threatening situation.

5. Location and Security of Computer Room - To reduce the risk of firing, the computer room should not be located in the basement or ground floor of a multi-storey building. Fireproof Walls, Floors, Ceilings surrounding Computer Room, & Office Materials should

have an adequate fire resistance rating. Less Wood and plastic should be in computer rooms.

6. Inspection by Fire Department - Regular (say annual) Inspection by Fire Department should be carried out to ensure that all fire detection systems act in accordance with building codes.

7. Norms to reduce Electrical Fires - To reduce the risk of an electrical fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit.

8. Exits - Fire exits should be clearly marked.

Water damage

1. Water Detectors - Computer rooms should have water detectors connected to alarms, to alert personnel that water is present in the facility. Water detectors should be placed under raised floors &t near drain holes.

2. Water leakage alarms - As much as computing systems dislike heat, they dislike water even more. Water leakage alarms must be placed at strategic points within the installation.

3. All ceilings, walls and floors should be waterproof.

4. An adequate water drainage system must exist to keep water away from equipment to prevent damage.

5. To reduce the risk of flooding, computer rooms should be located at the core of the building. Try to avoid locating these rooms on the ground floor, on the top floor, and in the basement whenever possible.

Types of Management Subsystems & Managerial Controls Change in Content

3. Systems Development Management - It is responsible for the design, implementation, & maintenance of application systems.

Systems Development Management Controls - Systems Development Management Controls help to ensure that proper documentations and authorizations are available for each phase of the system development process. These are given as follows:

1. Problem definition & Feasibility assessment - System development projects are undertaken when the user faces a problem in the existing system or to take advantage of opportunities arising from the new system. The steps in this phase are to understand the exact nature of the problem or opportunity; define the project scope and constraints; perform fact-finding; and evaluate feasibility. Feasibility study examines whether the project initiative is viable, or achievable, from financial, technical, and organizational standpoints.

2. Analysis of existing system - In this phase, data is collected about the present system. This data is then analyzed, & new requirements are determined. To determine requirements, analyst has to interact with all stakeholders to determine what is needed from proposed system.

3. Information Processing System design - In this phase, designers will map specific requirements into designs. This phase involvesfollowing activities:

1. Design of data/information flow by using tools like data flow diagrams (DFD).

2. Design of database (both local and global database).

3. Design of user interface to allow user to interact with the system.

4. Physical design from logical design.

5. Design the hardware/software platform

4. Hardware/software acquisition & procedures development - These include hardware acquisition, software acquisition or development (programming). The detailed hardware/software acquisition process includes the request for vendor hardware/software proposals and their evaluation.

5. Acceptance Testing and Conversion - Acceptance Testing is carried out to identify errors or deficiencies in the system prior to its final release into production use. The conversion means changing from one system (say old/manual) to another (new/computerized).

6. Operation and Maintenance - After passing testing stage, system is implemented in live/production area. New hardware if required is installed and users are trained. After

implementation, system is reviewed/maintained; it is modified to adapt to changing users ft business needs.

5. Data Administration (IMP) -Data administration is responsible for issues in relation to use of an organization's data.

Data Resource Management Controls - Data is a critical resource that must be managed properly, accordingly, centralized planning & control should be implemented. Data must be available to users when/where it is needed, and in the form in which it is needed. Data modification should be authorized, & the integrity of data should also be preserved. The control activities for maintaining integrity of the database is as under:

(1) Data Definition Controls - To ensure that the database always corresponds and comply with its definition standards.

(2) Existence / Backup Controls - Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are given as follows -

- **Dual recording of data -** Under this strategy, two complete copies of the database are maintained & they are concurrently updated.
- **Periodic dumping of data -** It involves taking a periodic dump of all or part of the database onto some backup storage medium.
- **Logging input transactions -** This involves logging the input data transactions which cause changes to the database.
- **Logging changes to the data -** This involves copying a record each time it is changed by an update action.

(3) Access Controls - To prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:

- **User Access Controls** through passwords, tokens and biometric Controls; and
- **Data Encryption -** Keeping the data in database in encrypted form.

(4) Update Controls - To restrict update of the database to authorized users in two ways:

- By permitting only addition of data to the database; and
- Allowing users to change or delete existing data.

(5) Concurrency Controls - These controls ensure the data integrity when two update processes access the same data item at the same time.

(6) Quality Controls - These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.

Auditors' Role in Data Resource Management Controls include the following -

I. Determine what controls are exercised to maintain data integrity and interview Database Users & Database Administrator to ensure that their roles and responsibilities are clearly defined.

II. Employ test data to evaluate whether Access Controls and Update Controls are working.

Boundary Controls (Slight Change)

The boundary subsystem establishes the interface between the would-be user of a computer system and the computer system itself.

For example, when a customer walks up to an automatic teller machine and begins the initial question-answer session during which the machine attempts to establish the identity and authenticity of the customer and what the customer wants to do, boundary subsystem functions are being performed. Boundary subsystem controls have one primary purpose: to establish the identity and authenticity of would-be users of a system. Once boundary subsystem functions are complete, the user can commence to use the resources of the system.

Boundary Control Techniques (Addition in Content)

Cryptography

1. Cryptography is defined as hiding the meaning of a message and revealing it at a later time. It is a an effective way of protecting sensitive information. It provides security for data in motion and at rest.

2. Cryptography transforms (encrypts) data into cryptograms (ciphertext). Clear text is the readable version of a message. After an encryption process, the resulting text is referred to as ciphertext.
3. The strength of the cryptosystem is depends on - the time & the cost to defeat the cryptosystem.

Access control

Access to system resources needs to be controlled. No individual should be able to log in to the system by using a level of authority higherthan their job requires. The Access Control Mechanism processes User'$ request for resources in 3 steps, namely; Identification, Authentication, Authorization

1. Identification - It describes a method of ensuring that an user is who he claims to be, Identification can be provided with the use of a username or account number.

2. Authentication - To be properly authenticated, the user is usually required to provide a second piece to the credential set. Users may provide 4 classes ofauthentication information as under;

(I) Remembered information - Name, Account number, passwords, PIN

(ii) Objects Possessed by the user - Badge, plastic card, key

(iii) Personal characteristics - Finger print, voice print, signature

These two credential items are compared to information that has been previously stored for this user. If these credentials match the stored information, the user is authenticated.

3. Authorization - It describes the actions the user can perform on a system once he has been identified & authenticated. Actions may include reading, writing, and executing files or programs.

Personal Identification Numbers (PIN)

A type of password (i.e. a secret number assigned to an individual by an institution) or customer selected number that verify the authenticity of the individual. Passwords/PINs are often shared, stolen, guessed, or otherwise compromised. Thus they are one of the weakest

authentication mechanisms. A PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission & storage.

Plastic Cards

Plastic cards are similar to credit cards that have microchips. The microchip, which is loaded with identifying data. Normally requires a PIN.

These cards are used to;

- Store information required in an authentication process and

- identify a user.

Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message. Digital signatures are especially important for electronic commerce and e-mail. Unlike a pen-and-paper signature, a digital signature can also prove that a message has not been modified.

Q Output Controls (Change in Content)

Output controls ensure that the results of data processing are accurate and complete and are directed to authorize recipients.

Additionally, access to reports should be based on a "need-to-know" basis in order to maintain confidentiality. A few output controls are;

Inference Controls - Often database contain information that is sensitive as individual rows, but not sensitive as a group. Inference controls ensure that information is released without disclosing personal information about a single individual. For example - Salary data across the company, individuals want their salary private, but knowing the average salary for each department is fine.

2. Batch Output Production & Distribution Controls - This includes several controls like;

- Storage Controls to ensure proper perseverance of output and appropriate inventory controls.

- Spooling file Controls for security of spooling output to a printer.
- Printing Controls to ensure that output is on correct printer without unauthorized disclosure of printed information.
- User output Controls to ensure that users review output on a timely basis;
- User/Client service Review Controls to ensure higher quality output and detection of errors or irregularities in output;
- Report program execution Controls to ensure that only authorized users are permitted to execute batch report programs;
- Report collection Controls to ensure that report is collected immediately and secured to avoid unauthorized disclosure.
- Report distribution Controls to ensure timely reports & a log for reports that were generated & distributed;

3. Batch Report Design Controls -Batch report design features should comply with the control procedures laid down for them during the output process.

4 Online output production & Distribution Controls - This includes several controls like;

- Retention Controls to evaluate for how long output is to be retained & deletion controls to delete the output once expired.
- Receipt Controls to evaluate whether the output should be accepted or rejected;
- Review Controls to ensure timely action of intended recipients on the output;
- Source controls to ensure that output which can be generated or accessed online is authorized, complete and timely;
- Communication Controls to reduce exposures from attacks during transmission;
- Distribution Controls to prevent unauthorized copying of online output when it was distributed. Actions that can be taken on the online output they receive.

Database Controls (Change in Content)

Database controls - Deal with ensuring an efficient & effective database system. It is critical that database integrity and availability are maintained. This is ensured through the following controls:

1. File Handling Controls - These controls are used to prevent accidental destruction of data contained on a storage medium.

2. Access Controls - Establish the necessary levels of access controls, including privileged access, for data items, tables and files to preventinadvertent or unauthorized access.

3. Concurrency Controls - Establish controls to handle concurrent access problems, such as multipleusers desiring to update the same data elements at the same time (i.e., transaction commit, locking of records/files).

4. Cryptographic Controls - These controls protect the integrity of data stored in the database using block encryption. (Already discussed under Boundary Controls)

5. Integrity Controls - Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database. It is important that these controls, if possible, be contained in the table/columns definitions. In this way, there is no possibility that these rules will be violated.

6. Application Software Controls - Many of these controls are provided by database management systems.

- **Update controls -** to ensure that only authorized personnel can update the database.
- **Report controls -**to identify errors or irregularities that may have occurred when the database has been updated.

Q- Communication Controls (Addition in (content)

Three major types of exposure arise in the communication subsystem -

1. Transmission impairments can cause difference between the data sent & the data received;

2. Data can be lost or corrupted through component failure; and

3. A hostile party could seek to subvert data that is transmitted through the subsystem.

Various communication controls are discussed below -

1. Physical Component Controls - These controls incorporate features that mitigate the possible effects of exposures on physical components such as Communication lines. Modem, Port protection devices. Multiplexers, and Concentrators etc.

2. Channel Access Controls - Whenever the possibility of contention for the channel exists, some type of channel access control technique.

3. Line Error Control - Whenever data is transmitted over a communication line, error because of attenuation distortion, or noise that occurs on the line must be detected and corrected.

4. Link Controls - Line error control & flow control are important to manage link between 2 nodes in a WANs.

5. Internetworking Controls - Different internetworking devices like bridge, router, and gateways are used to establish connectivity between homogeneous or heterogeneous networks. Therefore, several control functions in terms of access control mechanisms, security and reliability of the networks are required to be established.

6. Flow Controls - Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data.

7. Topological Controls - A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. The network must be available for use at any one time by a given number of users that may require alternative hardware, software, or routing of messages.

8. Controls over Subversive threats - Firstly, the physical barriers are needed to be established to the data traversing into the subsystem. Secondly, in case the intruder has somehow gained access to the data, the data needs to be rendered useless when access occurs.

Auditing The Application Control Framework

In case the external auditors have evaluated the reliability of management controis, the next step is to determine the adequacy of application controls. When performing an audit of application controls the information System auditor needs to assess the following key areas:

Auditing Boundary Controls -

When performing an audit of this area, the IS auditor needs to assess the following:

1. To determine whether adequate boundary controls are in effect to safeguard assets & preserve data integrity.

2. To determine whether access control mechanism implemented in the system is sufficient or not.

3. To understand which approach has been used to implement access control so that they can predict the likely problems.

4. To ensure that careful control is exercised over maintenance activities, in case of hardware failure.

5. To address three aspects to assess cryptographic key management –

(1) How keys will be generated? (2) How they will be distributed to users? (3) How they will be installed in cryptographic facilities?

Auditing Input Controls -

When performing an audit of this area, the IS auditor needs to assess the following:

1. To understand the well-designed source document that increases the speed and accuracy with which data will be captured, prepared &entered into the computer systems & how the document will be handled, stored & filed.
2. To examine the data-entry screens used in an application system to reduce common data-entry errors.
3. To evaluate the quality of the coding systems used in application system to determine their likely impact in the data integrity,effectiveness, and efficiency objectives.

4. To comprehend various approaches used to enter data into an application system and their relative strengths and weaknesses.
5. To check whether input files are stored securely and backup copies of it are maintained at an off-site location so that recovery remains unaffected in case system's master files are destroyed or corrupted.

Auditing Communication Controls -

When performing an audit of this area, the IS auditor needs to assess the following:

1. To examine and evaluate various controls in the communication subsystem.
2. To collect enough evidence to establish a level of assurance that data transmission between two nodes in a WAN is accurate & complete.
3. To look whether adequate network backup and recovery controls that strengthen network reliability are practiced regularly or not.
4. To assess the encryption controls to ensure the protection of privacy of sensitive data.
5. To assess the topological controls to review the logical arrangement of various nodes and their connectivity.

Auditing Processing Controls -

1. When performing an audit of this area, the IS auditor needs to assess the following:
2. To determine whether user processes are able to control unauthorized activities like gaining access to sensitive data.
3. To evaluate whether the common programming errors that can result in incomplete/ inaccurate processing has been taken care or not.
4. To assess the performance of validation controls to check for any data processing errors.
5. To check for the checkpoint and restart controls that enable the system to recover itself from the point of failure.

Auditing Database Controls

When performing an IS auditor needs to assess the following:

1. To check for the mechanism if a damaged or destroyed database can be restored in an authentic, accurate, complete, and timely way.
2. To comprehend backup and recovery strategies for restoration of damaged or destroyed database in the event of any failure.
3. To evaluate whether the privacy of data is protected during all backup and recovery activities.
4. To check for proper decisions made on the maintenance of the private and public keys used under cryptographic controls.
5. To assess data integrity and the ways in which files must be processed to prevent integrity violations.

Auditing Output Controls -

When performing an audit of this area, the IS auditor needs to assess the following:

1. To check for the mechanism if a damaged or destroyed database can be restored in an authentic, accurate, complete, and timely way.
2. To comprehend backup and recovery strategies for restoration of damaged or destroyed database in the event of any failure.
3. To evaluate whether the privacy of data is protected during all backup and recovery activities.
4. To check for proper decisions made on the maintenance of the private and public keys used under cryptographic controls.
5. To assess data integrity and the ways in which files must be processed to prevent integrity violations.

Auditing Output Controls -

When performing an audit of this area, the IS auditor needs to assess the following:

1. To determine what report programs are sensitive, who all are authorized to access them Et only authorized persons must execute them.

2. To review that the action privileges that are assigned to authorized users are appropriate to their job requirement or not.
3. To evaluate controls in terms of alteration of the content of printer file, number of printed copies etc.
4. To determine whether the report collection, distribution and printing controls are well executed in an organization or not.

Chapter 4.

E-Marketing Models

E-Marketing - Electronic marketing is a subset of - business. -Marketing is the process of marketing a product or service using the

Internet. Some e-marketing models are as follows:

1. Portal - A portal or Web portal is a site that people use as a launching point to enter the Web (the word "portal" means "gateway"). The services offered by most portals include a search engine, news, email, chat, forums, maps, shopping etc. Large portals include many additional services (e.g. Yahoo!).

2. e-Shop (electronic shop/e-tailers) - -shop sometimes called e-tailing /e-retailing is the direct sale from business to consumer through electronic storefronts, typically designed around an electronic catalogue and shopping cart model. For example: www.dell.com.

3. e-Mall (electronic mall or digital mall/ cyber-mall) - An e-mall, in its basic form, consists of a collection of e-shops usually grouped under asingle Internet address. It is a website that displays electronic catalogue from several suppliers, and charges commission from them for the sales revenue generated at that site. This store could be a specialized or generalized e-store.

- **General e-stores/malls:** Generalized e-stores sell a large number of product lines rather than confining themselves to just one or a very few product lines. It includes store like amazon.com which is primarily an e-mall that provides platform to vendors

sell and users to purchase various products ranging from books, music, movies, housewares, electronics, toys, clothes etc.

- **Specialized e-stores/malls:** Specialized stores would sell only specialized items. E.g, specializes in buying & selling property & housing on an online platform.

4. E-auctions (electronic auctions) - In it, bidding for goods and services can be performed with the help of electronic implementation. This method of auction is less time consuming and convenient for both suppliers and buyers. eBay (www.ebay.com) is the best-known example and offers both B2B and B2C offerings.

5. Buyer Aggregator - Buyer Aggregator pools many buyers together to drive down the price of selected items. The individual buyer, thus, receives the price benefit of volume buying. The more buyers that join the pool, the lower the price drops, usually.

Q Different Types of Digital Payments -

9. e-RUPI

1. What is e-RUPI? - e-RUPI is a cashless and contactless payment mechanism. e-RUPI is a QR code or SMS string-based e-voucher, which is delivered to the mobile phones of the beneficiaries. e-RUPI voucher is a pre-paid voucher, which beneficiary can go and redeem it at any centre that accepts it. Any government agency and corporation can generate e-RUPI vouchers via their partner banks. Eleven banks are currently live with the service.

2. e-RUPI Vouchers are Person & Purpose & Service-Specific - e-RUPI connects sponsors of the services with beneficiaries & service providers in a digital manner. For example, if Government wants to cover a particular treatment of an employee in a specified hospital, it can issue an e-RUPI for the determined amount through a partner bank. The employee will receive a SMS or a QR Code on his/her feature phone/ smartphone. He/she can go to the specified hospital, avail of the services, & pay through the e-RUPI voucher received on his/her phone.

3. Who can use e-RUPI? - Many services can be provided by the government through e-RUPI in the country. e-RUPI removes the middlemen and there's no direct cash involved. e-RUPI expected to ensure a leak-proof delivery of welfare services & minimize fraud & corruption.

The gains of the e-RUPI ecosystem are not restricted to public service delivery only. The voucher can also be used by private organisations to provide benefits to their employees and undertake corporate social responsibility (CS) activities. For Example -The corporate sector may use e-RUPI to issue vouchers for various employee benefits like meal vouchers, transport allowance, vaccination, etc. If any organization wants to help someone in their treatment, education or for any other work, then they will be able to give an e-RUPI voucher instead of cash. Someone in their treatment, education or for any other work, then they will be able to give an e-RUPI voucher instead of cash.

4. Benefits of e-RUPI - This contactless e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential. e-RUPI voucher is only available for one-time use and does not require any plastic card, internet banking or mobile application. The voucher can be redeemed using both smartphones and feature phones. e-RUPI assures timely payment without involvement of any Intermediary. These vouchers are person- and purpose-specific, meaning that e-RUPI voucher issued for vaccine can be redeemed only for that.

Q| Blockchain& Its Applications and related Risks and Controls

1. What is Blockchain? - Blockchain is a an open, distributed electronicledge that is shared by all participants in the network. It is resistant to any modifications. Blockchain is also called Distributed Ledger Technology (DLT).

2. How Blockchain Works? - Blockchain is a new way of sharing and storing information where many people can add entries and a community of users control how it is updated. In this technology, transactions are recorded to the ledger as a block, and each block is attached to the previous block in the chain in chronological order. When a new block of transactions is created, a new block is added to the chain. A constantly updated list of blocks is given to everyone who participates. Once recorded, a blockchain transaction cannot be changed due to the fact that the same transaction is recorded over multiple, distributed databases. To change any record in the blockchain, one must change every subsequent block. Everyone in the blockchain has access to all the data in the blockchain. The data itself is encrypted and private, but the technology and ledger are completely open.

A simple analogy for understanding blockchain technology is a Google Doc. When we create a document and share it with a group of people, the document is distributed instead of copying or transferring it. This creates a decentralized distribution chain that gives everyone access to the document at the same time.

3. Benefits of blockchain-based transactions - Blockchain-based transactions are transparent, tamper-proof, and stored on multiple servers. If any data in the chain were to be altered, it would be painfully obvious to everyone in the chain that someone tried to alter it.

4. Application of Blockchain Technology - There are numerous applications of blockchain technology. We list a few here.

- **Travel Industry -** Blockchain allows tourists to store information about their movements, purchases & visits to attractions in a single place. In the case of a travel agency booking flights and hotels for a customer, it has to send the information to the different firms.
- **Healthcare -** Better data sharing between healthcare providers means a higher probability of accurate diagnoses, more effective treatments, and the overall increased ability of healthcare organizations to deliver cost-effective care.
- **Economic Forecasts -** Good forecasting requires quality analysis of data from various sources, both internal and external. Blockchain provides a valuable and trusted data source that planners can use for better financial and economic forecasts and insight.
- **Government -** Most government departments work in silos. The lack of interconnectedness across departments is not desirable for data integrity & consistency. Blockchain technology has the potential to make government operations more efficient.
- **Financial Services -** In traditional finance, clean audit trails/logs can be difficult to procure at times, which have led to severe economic losses in the past due to negligent behaviour or malicious actors. Blockchain has the potential to make the financial services industry more transparent, less susceptible to fraud and cheaper for consumers.

5. Risks and Controls relating to Blockchain -

Risks-

- With the use of blockchain, organizations need to consider the risks with a broader perspective. Who is or is not responsible for managing the risks, its proper accountability should be set in the blockchain.
- The reliability of financial transactions is dependent on the underlying technology and if this underlying consensus mechanism is tampered with, it can make financial information inaccurate and unreliable.
- The central authority has to administer Et enforce the amendments, otherwise process control activities may be challenged.
- Blockchains involve huge amounts of data that are updated frequently, so the risk of information overload can be a challenge.

Controls

- Since blockchain contains a large amount of data that is frequently updated, computerized continuous monitoring techniques must be used to conduct ongoing evaluations.
- Appropriate data analysis procedures should be developed to identify and obtain relevant data for business processes E reporting objectives of the management.
- Communication methods should be developed to ensure that operational changes and updates relating to the use of blockchain are communicated to appropriate personnel
- Unique aspects of blockchain such as consensus protocols, smart contracts, and private keys, etc. should be assessed thoroughly.
- Both internal and external auditors must be engaged in discussions during the development or identification of a blockchain so as to make the management understand the typical auditability issues associated with using blockchain.

Chapter 5

Q Cyber Security Framework Prescribed by RBI for Banks –

RBI has released a guideline for cyber security framework specially designed for Banks. Some key features of Cyber Security Framework as prescribed by RBI for banks are as under:

(A) Network Security and Secure Configuration - The following key measure are required to be implemented:

1. Identification of the risks - to ensure that risks are within the bank's risk appetite and are managed appropriately.

2. Different LAN segments - for in-house/onsite ATM and CBS/branch networks to confirm the adequacy of bandwidth to deal with transaction volume so as to prevent slow speed and resulting low efficiency.

3. Use of routers, hubs and switches - to ensure secure network configuration.

4. Multi-layered boundary defines -detection systems - to protect the network from any malicious attacks and to detect any unauthorized network entries.

5. Periodic security review of systems and terminals - to assess the network's vulnerability and identify the weaknesses.

B) Application Security - Full-fledged Security to ensure Confidentiality, Integrity and Availability (CIA) of data and information needs to be development and implemented covering following key features:

1. Bank Specific Email Domains - Implementation of bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti- phishing (security measures to prevent steal of user data) and anti-malware software (software tool/program to identify and prevent malicious software/malware from infecting network) with controls enforced at the email solution.

2. Audit Log Setting - Capturing of the audit logs pertaining to user actions and an alert mechanism to monitor any change in the log settings.

3. Two factor authentication - An extra step added to the log-in process, such as a code sent to user's phone or a fingerprint scan, that helps verify the user's identity and prevent cybercriminals from accessing private information.

4. Password Management Policy - Implementation of Password Management policy to provide guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.

5. Reporting mechanism - Proper reporting mechanism to save the banks from the effects of misconduct - including legal liability, lasting reputational harm and serious financial losses.

6. Effective Change Management Process - Effective change management process to record/ monitor all the changes that are moved pushed into production environment.

7. Due Diligence and Oversight - Conduct effective due diligence and oversight to thoroughly assess the credentials of vendors/third party service providers/partners and making non-disclosure and security policy compliance agreements mandated for them.

8. Incident response and management mechanism - to take appropriate action in case of any cyber security incident with well written incident response procedures elaborating the roles of staff handling such incidents.

9. Configuration Management Processes - Robust configuration management processes to register changes to business applications, supporting technology, service components and facilities.

10. Training of employees - to educate them to strictly avoid clicking any links received via email.

11. Surveillance Mechanism - Continuous surveillance to stay regularly updated on the latest nature of emerging cyber threat.