PAPER 6

CA FINAL COURSE

INFORMATION SYSTEMS CONTROL AND AUDIT

SOME WORDS FROM CHANAKYA:

-- One can conquer a greedy by money, an arrogant by politeness, a fool by fooling & a learned by truth.

-- Money is best protected in charity. The water of pond stays good if it has inflows and outflows.

SOME WORDS FROM ROBIN SHARMA:

-- Associate with positive & focused people

-- You must have mission statement in your life.

-- Remember people's name & treat everyone well.

PREPARED BY

CA AKHIL MITTAL
ACA, B.COM (H)
E-MAIL ID: caakhil24.srcc@gmail.com

CHAPTER: 9 (AS PER ICAI)

DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING

1.) IMPORTANCE OF INFORMATION SYSTEM SECURITY:

In today's world, all the information travels through cyberspace on a routine basis, the significance of information is widely accepted. Organization depends on timely information. So it is imperative that organization must have strong information system.

But there are various risks associated relating to information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by:

CODE TO REMEMBER: E^2 – D.I.E.T

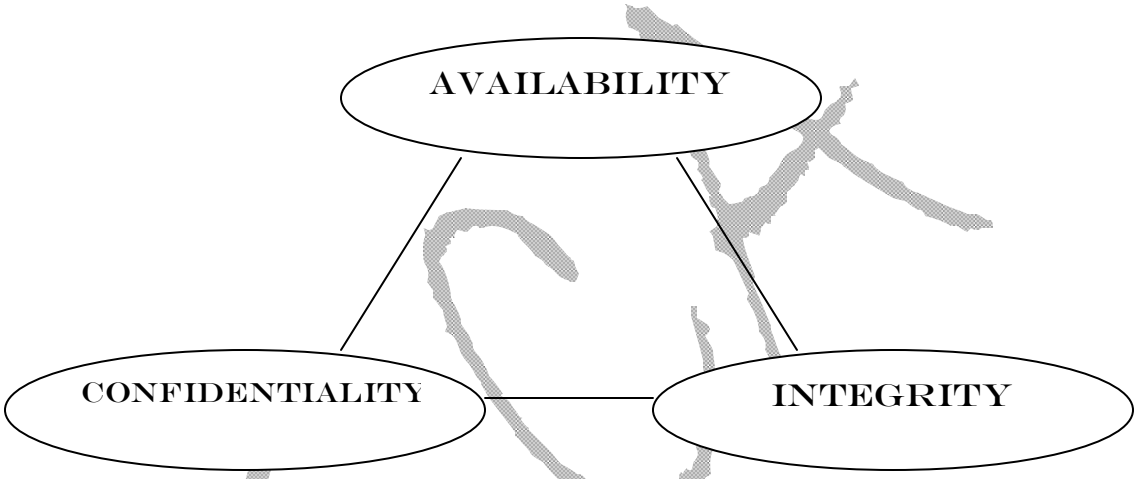
1.) **E**limination of distance, time & space as constraints.
2.) **E**lectronic attacks
3.) **D**evolution of management and control
4.) **I**nterconnectivity of systems
5.) **E**xternal factors such as legislature, legal & regulatory requirements or technological developments.
6.) **T**echnology usage is worldwide.

Adequate measures for information security help to secure the smooth functioning of information system and protect the organization from loss or embarrassment caused by security failure.

2.) INFORMATION SECURITY:

SECURITY means **protection** & **INFORMATION SECURITY** means **protection of information.** The objective of the information system is **"the protection of the interest of those relying on information and information system & communication that deliver the information free from harms, from failure of availability, loss of confidentiality & integrity.**

OBJECTIVE OF INFORMATION SECURITY (C.I.A)



THIS IS ALSO THE PURPOSE & SCOPE OF INFO. SECURITY POLICY

CONFIDENTIALITY: Data & information are disclosed only t those who have a right to know it.

INTEGRITY: Data & information are protected against unauthorized modification.

AVAILABILITY: Information systems are available & usable when required.

3.) WHY INFORMATION SECURITY IMPORTANT:

- For smooth functioning of business activities since easy availability of data.
- Organization must ensure that all users are given required information by providing secure information system environment.
- Ensures smooth functioning of information system & protect the organization from loss caused by failures.

4.) WHAT KIND OF INFORMATION IS SENSITIVE:

Factors considered for deciding level of protection needed fro information:

CODE TO REMEMBER: F.B.S (Fake Balance Sheet)

A.) FINANCIAL INFORMATION:

Financial information such as salaries, wages customer orders position, cash & bank positions etc are very crucial and should not be made public or disclosed. When a competitor knows specific information about a company's wages, he may be able to price its product accordingly. As such, the damage to the organization may be significant.

B.) BUSINESS OPERATION INFORMATION:

It consists of an organization process and procedures which are related to production & technologies which are proprietary in nature. And it is necessary to secure this type of information. While most of the organization prohibits the sharing of data, any type of carelessness may result in inadvertent (negligent) storage of data on authorized systems, unprotected laptops and failure of secure magnetic media.

C.) STRATEGIC PLANS:

Strategic plans are very crucial for success of organization and it is required that these strategic plans should be well protected. These plans normally involves the decision making part of the management. For instance a company discovers new areas of launching its product, but due to weak information security system the same is being exploited by its competitors. This may result in loss to the former company

5.) FACTORS DECIDING LEVEL OF SECURITY NEEDED FOR INFORMATION:

CODE TO REMEMBER: V-SOAP

A.) Value of information:

- All the information is not same in nature& to be handled accordingly.
- Timely availability of the information is vital in better decision making.
- Level of information security depends on the value of information.
- For e.g. Papers having nature of confidentiality must be secured properly as compared to information used on daily basis.

B.) **S**torage Media Type:

- Storage media is very crucial aspect fro deciding security level.
- If information is vital & confidential it has to be secured properly
- For instance non vital can be stored in floppy disks, & vital information can be stored on a hard disk or on some secured backup facility area.

C.) Output (Hardcopy of information):

- The output of employee's daily work must be reviewed.
- & decision has to be taken on the level of security.
- It includes various issues like what safeguards measures are placed for the drafts & working papers.

D.) Access to information:

- Who should be provided access to information and upto what level.
- Data which is very important and crucial should be provided enough security not only for accessing but also to DATA Files containing information buy using proper access control mechanism.

E.) Place of critical data:

- How the information is placed is critical factor i.e. whether on server or in a computer protected with password.
- If information is spread over at various places then an integrity security solution should be provided for company data & information.

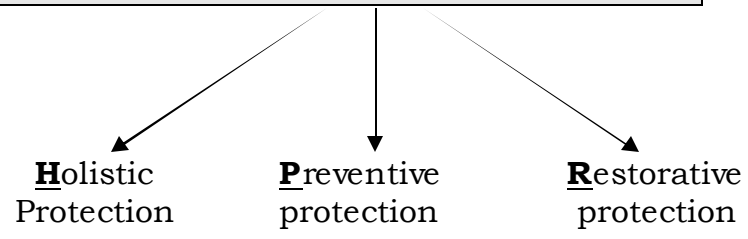
6.) CORE PRINCIPAL OF INFORMATION SECURITY :

CODE TO REMEMBER: MICS – RATA (CRAM MICS)

Multidisciplinary	Security must take into consideration both technological & non-technological issues.
Integration	Security must be coordinated & integrated. The policies iro security must be integrated with other functions.
Cost Effectiveness	Security must be cost effective. Security provided should be properly evaluated in terms of cost and benefits.
Society Factors	Ethics must be promoted by respecting the rights & interest of others.
Reassessment	Security policies must be reassessed periodically. It should be assessed from time to time.
Accountability	Information security requires a proper accountability among data owners, process owners & users etc.
Timeliness	Security procedure must monitor & provide timely response on case of any breach of information security.
Awareness	Awareness of risks & security initiatives must be properly communicated among all. Security measures will be effective if persons involved are aware of risk.

7.) INFORMATION PROTECTION METHOD:

CODE TO REMEMBER: H.P.R



A.) Holistic Protection:

- Protection must be done holistically and give the organization the appropriate level of security.
- One must be prepared for the unexpected & unknown and worst event to happen and immediately recover from these events, if they occur.

B.) Preventive Protection:

- This is based on use of security controls. This is generally based on 3 types of control:

  -- **Logical Controls:** Password, file permission, access control etc.

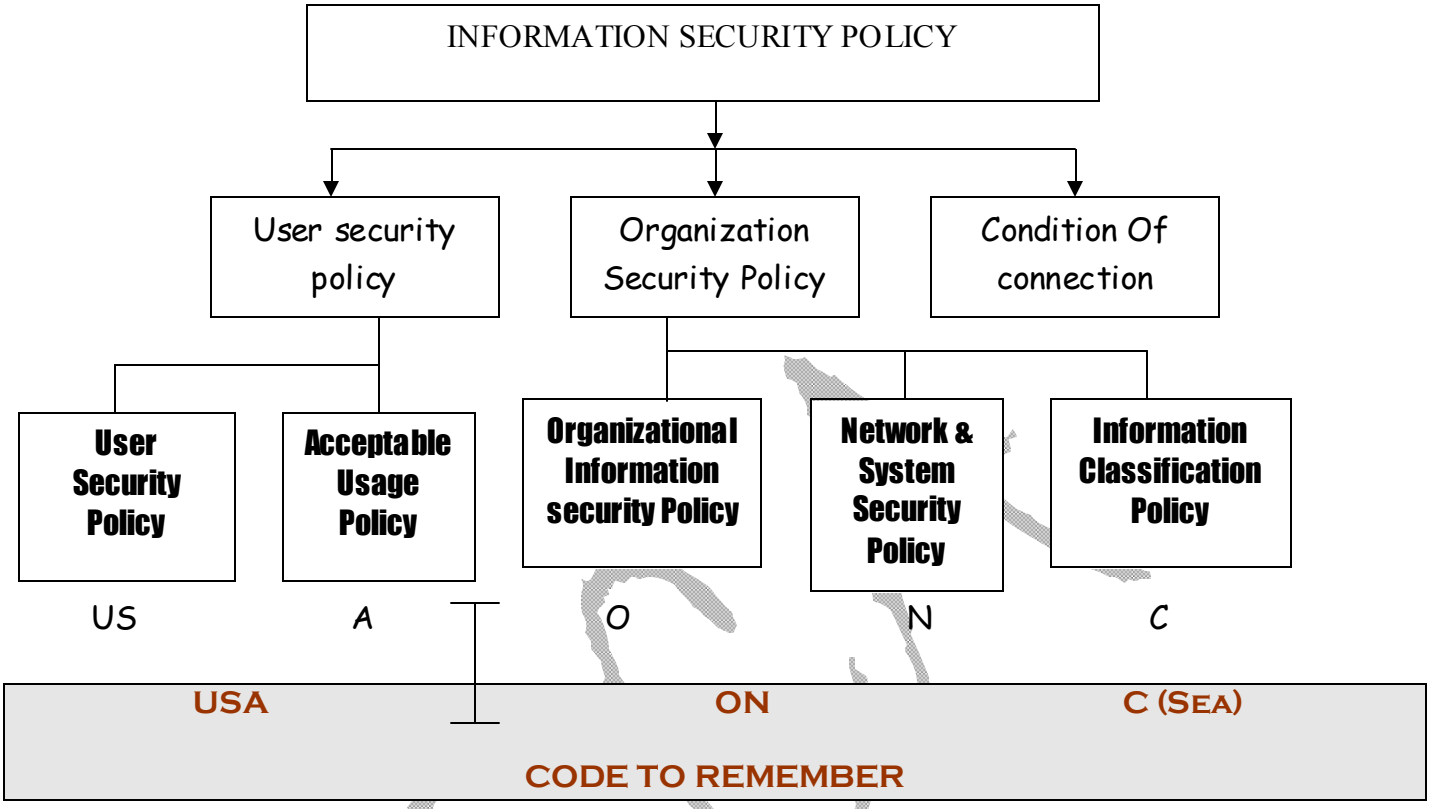
  -- **Administrative Controls:** Security awareness, policy, training.

  -- **Physical Control:** Doors, locks, Access lock, CCTV etc.

C.) Restorative Protection:

- Events that damage the information will happen, so, it is necessary to have an effective and timely information backup & recovery plan.
- Organization normally feels that restorative protection means **just to take the backup of data.** The recovery plan should be with proper planning considering the following issues:
  - How long it takes to recover the destroyed data by using backup of data.
  - Is recovery processes have been tested before?
  - How much productivity will be lost in backup is this acceptable? **etc**

8.) TYPES OF INFORMATION SECURITY POLICIES & THEIR HIERACHY:



1.) Use Security Policy: This set out the responsibilities & requirements from information system User.

2.) Acceptable Usage policy: this policy defines **rules** for use of **email & internet services.**

3.) Organizational information security policy: This policy defines group of policies for security of its information assets & IT system.

4.) Network & System Security Policy: This policy defines **rules for network & data communication security.**

5.) Information Classification Policy: This policy defines rules for **classification of information.**

6.) Condition Of connection: This policy defines the **rules for access of network** & it also specifies the conditions to be **satisfied for connection to networks.**

9.) INFORMATION SECURITY POLICY:

A POLICY is a plan or course of action, designed to influence and determine decisions, actions & other matters. It is a set of law, rules and practices that regulates how sensitive information, assets are to be protected.

An information security policy must define the following in detail :

☑ **ISSUE TO ADDRESS :**

- A definition of information security
- Why information security is important
- Goals & principles of information security
- Brief description of various information security standards
- What information needs the protection
- Reference to supporting documents used.

☑ **ROLES & RESPONSIBILITIES OR MEMBERS OF SECURITY POLICY:**

- **Management:** Members who have budget & policy authority.
- **Technical:** Members who know what technically can be supported.
- **Legal:** Experts who know the legal consequences of various rules.

The following should be studied from ICAI module or Dinesh Madan:

1.) **Access Control**
2.) **Incident Handling**
3.) **Physical & environmental Security**
4.) **Business Continuity management**

It's my humble request to you all that don't cram these topics. If possible please make small notes of these and then study.

10.) AUDIT POLICY:

The audit policy provides the guidelines to the audit team to conduct an audit son IT based infrastructure system.

Following are the threats that are addressed by the IS audit:

CODE TO REMEMBER: I & VO- U.P.A
Means I (me) & Vo (that) – UPA (govt. name)

1.) **I**nformation (confidential data) access by the unauthorized person.

2.) **V**irus infections

3.) **O**pen ports/ unrestricted modem ports may be accessed by an outsider

4.) **U**nauthorized access of the department computers.

5.) **P**assword disclosure compromises.

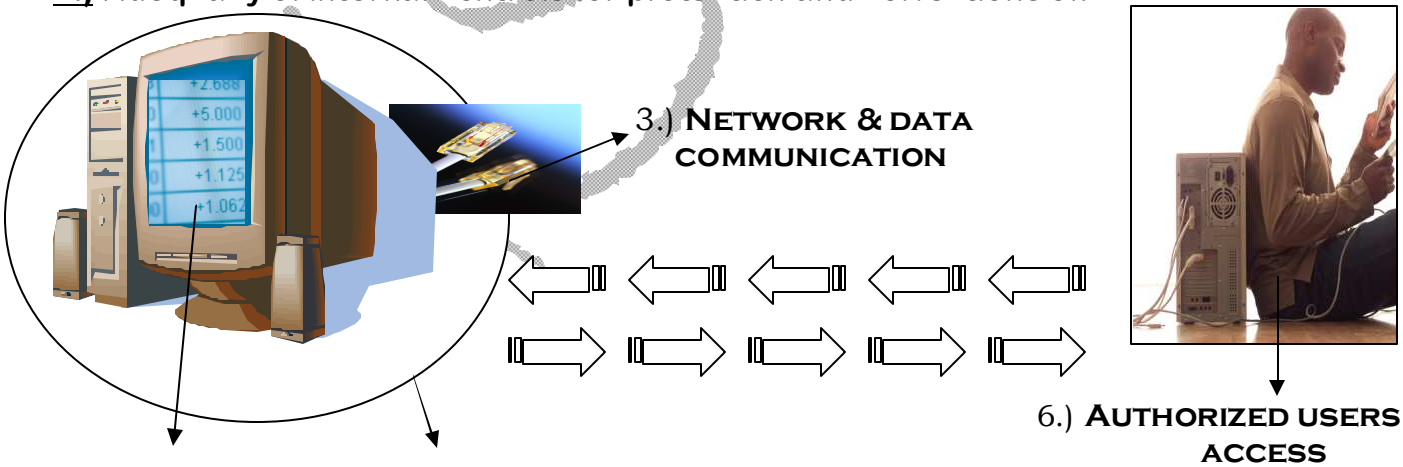
6.) **A**ttacks

11.) SCOPE OF IS AUDIT POLICY:

It includes the **examination and evaluation** of the **adequacy and effectiveness** of the **internal controls.** Following are the included as a part of IS audit scope:

CODE TO REMEMBER: BELOW GIVEN DIAGRAM

1.) Adequacy of internal controls for protection and corrections of:



In addition to above scope, IS audit also includes:

CODE TO REMEMBER: C.O.B.R.A

1.) **C**ompliance of the organization i.r.o the information system & security policy rules.

2.) **O**utput is meeting the required goals & objectives.

3.) **B**usiness continuity plan/ disaster Recovery plan must be appropriate.

4.) **R**isk & threats have to be determined in respect of information system.

5.) **A**cquisition/procurement of system must be evaluated properly.

12.) WHAT AUDIT POLICY DO:

The audit policy should lay down the **responsibility of audit.** The audit may be conducted by internal/external auditor. It (proper audit) is achieved through **organizational status & objectivity.**

- ☑ The policy should lay out the **periodicity** of the reporting.
- ☑ A statement of **professional proficiency.**
- ☑ All information system auditors will sign a declaration of faithfulness & secrecy before commencing audit work in a form.
- ☑ The policy lay out the extent of testing to be done under various phases of audit:

  -- Planning

  -- Compliance Testing

  -- Substantive Testing

13.) AUDIT WORKING PAPERS & DOCUMENTATION:

WORKING PAPERS:

Working papers includes:

-- The audit plan
-- The Nature of audit
-- Timing of audit
-- Details on auditing procedures performed
-- Conclusions drawn from the evidence obtained

In case of recurring audit, working papers may be classified as PERMANENT such as:

CODE TO REMEMBER: I- B.I.A.S

1.) **I**S polices of the organization.

2.) **B**ackground of the information system in the organization

3.) **I**nternal control records related to information system.

4.) **A**udit report copes and observations of earlier years.

5.) Structure of the organization.

DOCUMENTATIONS:

Planning Documentation	Finalizing Documentation
The auditor should plan his final documentation to be based readers of documents. Following are the key factors n planning documentations: **1.) Knowing you resources:** Time,people, Money **2.) Knowing your audience:** **3.) Knowing your Scope:** complete audit scope.	Before distributing the documents to its reader the document should be in good profession form. **1.) Document to be thoroughly reviewed.** **2.) Document must have index & glossary.** **3.) Document to be properly formatted.**

14.) CONETNT OF IS AUDIT REPORT:

IS audit report is an end product of information system audit, conducted by an IS auditor. This report is communicated to management with opinions. Though there is no standard format or guidelines for preparation of this report, but overall this report may have the following:

CODE TO REMEMBER: TCS/I/FOA

- **T**itle & cover page.
- **C**ontent table
- **S**ummary(table)
- **I**ntroduction:
  - -- Background of IT environment or context
  - -- Purpose of audit
  - -- Scope of audit
  - -- Methodology used for auditing
- **F**indings
- **O**pinion
- **A**ppendices

IN THE END IT'S MY REQUEST TO ALL OF YOU THAT DON'T IGNORE THIS SUBJECT. IS IT POSSIBLE FOR YOU TO CLEAR CA WITHOUT PASSING IN THIS SUBJECT???? IF YOU FACE ANY PROBLEM IN MY NOTES DO LET ME KNOW SO THAT I CAN MAKE CORRECTIONS IN IT.

ALSO IN THIS CHAPTER I LEFT SOME OF THE TOPICS WHICH I HAVEN'T STUDIED. SO ALSO DO REFER THOSE TOPICS IF YOU WANT.