20CB504

Hall Ticket Number:

III/IV B.Tech (Regular) DEGREE EXAMINATION

February,2023 — **Cyber Security**

Fifth Semester — **Introduction to Information Security & Cyber Laws**

Time: Three Hours — **Maximum:** 70 Marks

Answer Question No. 1 Compulsorily. (14X1 = 14 Marks)

*Answer **ANY ONE** question from each Unit.* (4X14=56 Marks)

1.	a)	What are the main components of Information system model? Input, Process, Output	CO1	L2	1M
	b)	Name three goals of Information Security. integrity, confidentiality and availability.	CO1	L1	1M
	c)	What is sandboxing in cyber security? client side security of applications (restricting rights of executing programs).	CO2	L1	1M
	d)	What are the security activities involved in each phase of SDLC? Description, output, synchronization, interdependencies	CO3	L2	1M
	e)	Which are very important in designing a secure system? ▪ SDLC has 5 phases Initial Phase, Development Phase, Implementation Phase, Maintenance phase, Disposal Phase	CO3	L3	1M
	f)	What is the ISO standard for developing enterprise-level security standard? ISO/IEC 27002:2005	CO4	L2	1M
	g)	Which act aims at the regulation of the use of IT? ISO/IEC 13335 (IT security management), IT Act 2000	CO4	L2	1M
	h)	What is cyber security? Cyber Security is the protection of information and information systems against the potential threats on the internet	CO1	L2	1M
	i)	What is the importance of encryption in Information Security? secrecy	CO2	L1	1M
	j)	How digital signature is formed? A mathematical approach used for authenticating a digital message or a document. A digital signature is a block of code, which authenticates the sender and assures the integrity of data. **Components of Digital Signature**	CO2	L2	1M
	k)	List Backup Security measures. Assigning responsibility, authority and accountability, Assessing risks, Developing data protection process, Communicating the process to the concerning people, Executing and testing the process	CO3	L3	1M
	l)	What are the components involved in the risk management process? **Framing, Assessing, Monitoring, Responding**	CO3	L2	1M
	m)	List threats to e- commerce. Privacy, Integrity, Authentication, Non-repudiation	CO2	L2	1M
	n)	What is software license? ▪ Software license is about the use or redistribution of s/w. ▪ Two categories of s/w licenses: 1) Proprietary 2) free and open source.	CO4	L3	1M

Unit -I

2.	a)	Write about Information Security along with web services. It is the process of securing, protecting the information from an unauthorized access, use and modification.	CO1	L1	7M 4,3

Organizations need to preserve data integrity, privacy and availability.
The password protection method is the basic level of security for information.
There are several programs, such as viruses and bugs, which are used to hack the password of a computer system or network.
The main goals of information security are integrity, confidentiality and availability.

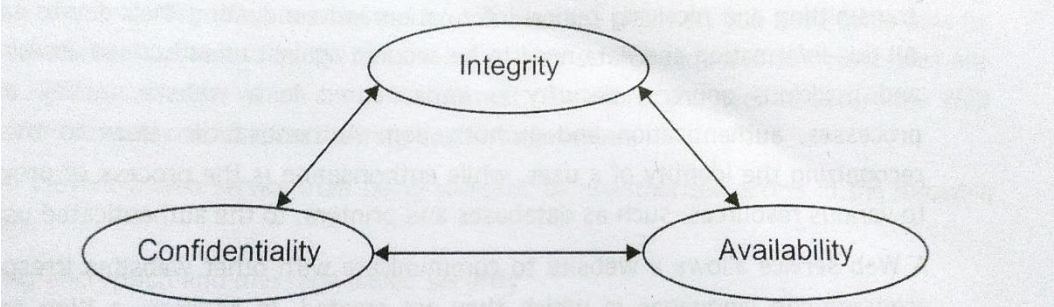


Figure 10: Displaying the Relationship between Goals of Information Security

- Confidentiality
- Process of securing information from unauthorized access.
- Ex: Credit card transaction, card number transmitted in encrypted form.
- Integrity
- Process of securing the information from unauthorized modification.
- Data integrity and data accuracy are related to each other.
- Availability: Information must be available when it is needed.

- **Role of Security in Internet and Web Services**
- Internet is used for exchanging data, online shopping, bank transaction, …
- Government organizations, businesses depend on internet.
- Data need to be secured against unauthorized access.
- Websites implement security mainly using i) authentication, ii) authorization
- Authentication: Recognizing the identity of an user.
- Authorization: Providing access to various resources to authenticated users.
- A Web Service allows a website to communicate with other websites irrespective of the programming languages.
- A Web Service can be accessed by any application, regardless of software and hardware platforms.
- A Web Service complies with SOAP, Simple Object Access Protocol and WSDL Web Service Description Language.
- A Web Service contains the logic for providing specific services to its consumers.
- A Web Service provides the abstraction between the consumer(client) and the provider.
- A Web Service only needs information about input, output, location of the client and Web Service provider.
- Before Web Services, developers used COM Component Object Model and DCOM Distributed Component Object Model.

❑ Advantages of Web Services over COM and DCOM:

- Web Services are simple to use, can be implemented on varied platforms.
- Web Services are loosely coupled, can be extended.
- Web Services do not carry state information, multiple requests can be handled simultaneously.
- COM, DCOM need to be physically distributed and explicitly registered on each client machine, which is not required for Web Services.

❑ **Securing Web Services**

- Web Service requests and responses are sent as XML documents
- Two ways of securing them:

1. Using encryption and message based security
2. Using authentication and access controls.

Encryption and message based security
Any modification done(by others) can be easily detected
Authentication and access controls
Validating a user against user credentials (user ID/password)

b) What is the need for Information security and explain different threats on IS. CO1 L3 7M 5

Need for Information Security

- Need to apply certain policies, measures and procedures in organizations, to maintain confidentiality, integrity and availability.
- These are available in ISMS: Information Security Management System.
- Organization should design, implement, and maintain a logical set of processes for managing threats.

Benefits of ISMS

- Maintains the security of the data and information.
- Protects the confidentiality, integrity and availability of data.
- Provides effective organization management.
- Effective and efficient data utilization possible
- Cultivates a sense of responsibility and accountability in the employees.
- Clients belief will be more and possibility of more investments.

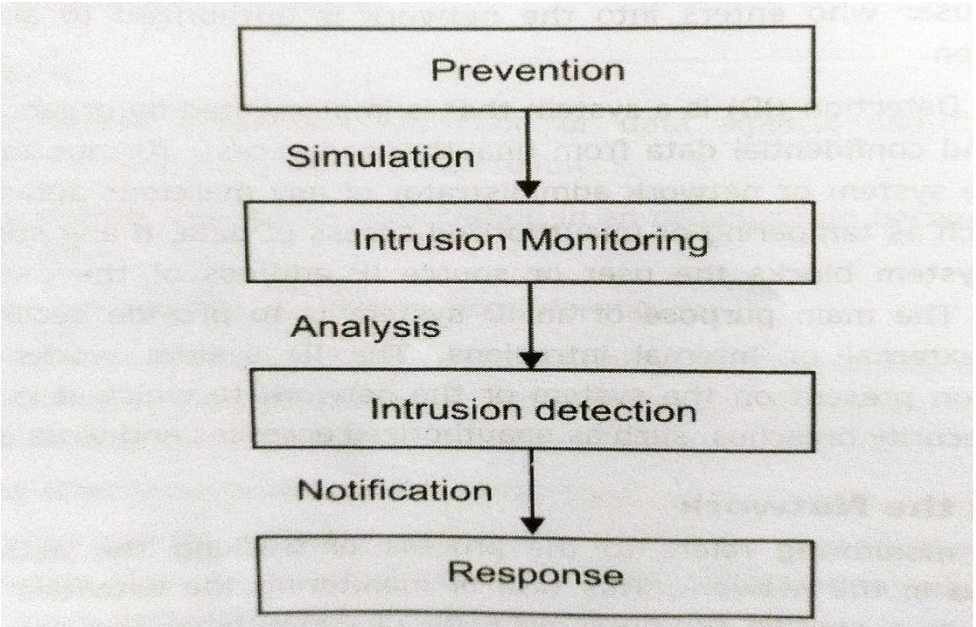
Security Implication for Organizations

- Security is ensuring the integrity, availability and confidentiality of data and resources against threats, viruses, bugs and vulnerability.
- The main components of a computer where an attacks can take place are software, hardware and data.
- Security is divided into 2 categories, 1. computer security(single), 2. network security(group).
- Network administrator should take care of passwords, firewalls settings.
- Identification, authentication can be used to secure.

Monitoring the Network

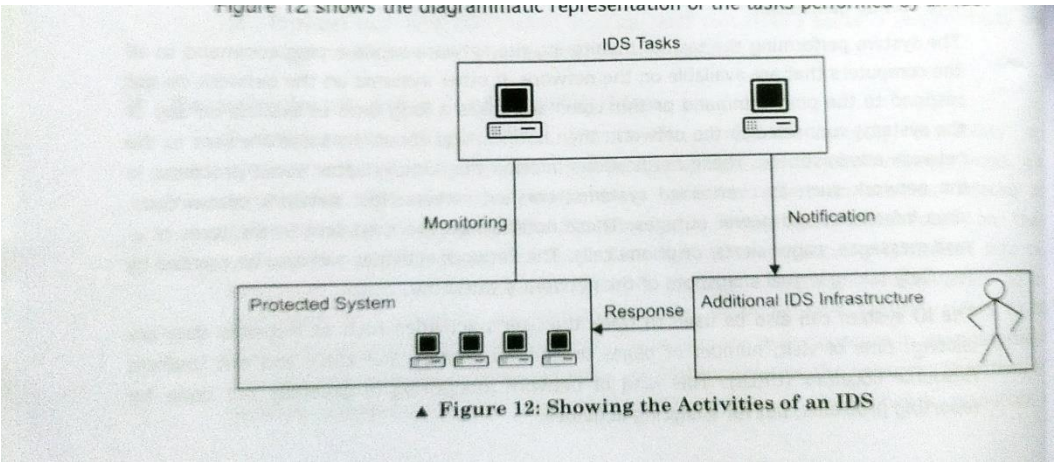
- Tracking the activities 24/7 in the network by a computer or set of computers.
- Needs strong backup power.
- This system keeps pinging all computers in the network.
- Depending on response, it detects problems like overloaded systems, crashed servers, lost network connections, virus infections, power outages, …
- The network activities can also be tracked by regularly taking virtual snapshots of the network's workflow.
- Users activities also can be tracked (which websites being visited, …)

Understanding Intrusion Detection System (IDS)



▲ Figure 11: Showing the Sequence of the IDSActivit

- **Understanding Intrusion Detection System (IDS)**



▲ Figure 12: Showing the Activities of an IDS

Threats to Information Systems 2

- A threat is an illegal activity, that can cause damages such as loss of information and data corruption.
- Two kinds of threats: 1. Accidental, 2. Intentional.
- Attacks can breach the security, two kinds of attacks: 1. Passive, 2. Active

Passive

- The attacker doesn't intend to harm the system.
- Observes the data to which the attacker doesn't have access rights.
- Three types of passive attacks:
  - Brute force attack: Breaks the encryption of data by finding the appropriate key.
  - Algebraic attack: Write a cipher as a system equation and read encrypted data using an appropriate key.
  - Code book attack: Builds a code book containing cipher text and corresponding plain text.

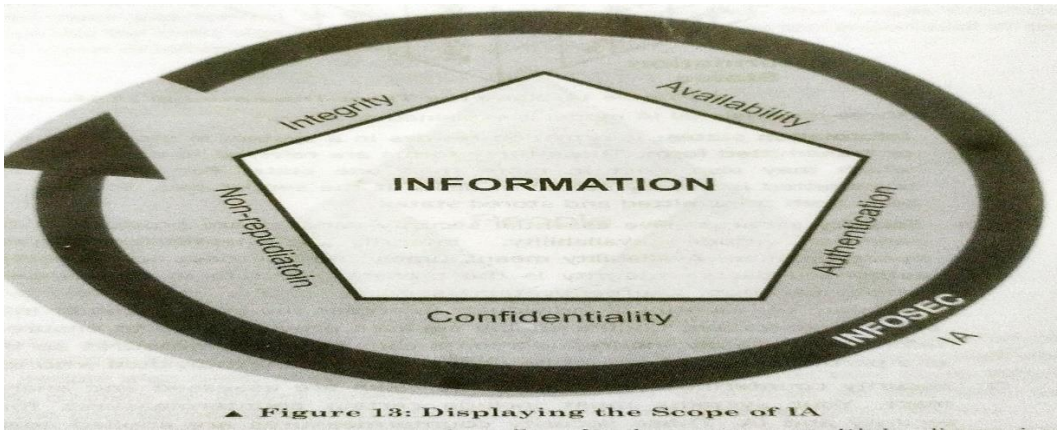
Active: Attacker with a bad intention to steal, create, delete, modify,… data.

(OR)

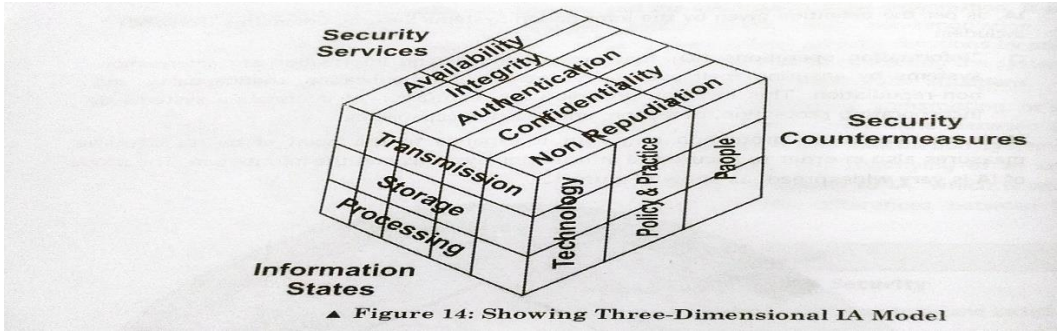
3. a) What is Information Assurance? explain with diagrams. CO1 L2 7M

Differences between IA and Information Security

- Management of risks associated with the Information System.
- It ensures availability, integrity, confidentiality, authentication and non-repudiation of an organizations information.
- Management of risks in processing, transmitting, storing of data.
- Information Security protects information from accessing, misusing, disclosing, disrupting, destructing and modifying in an unlawful manner.
- IA includes number of disciplines which includes Information Security also.

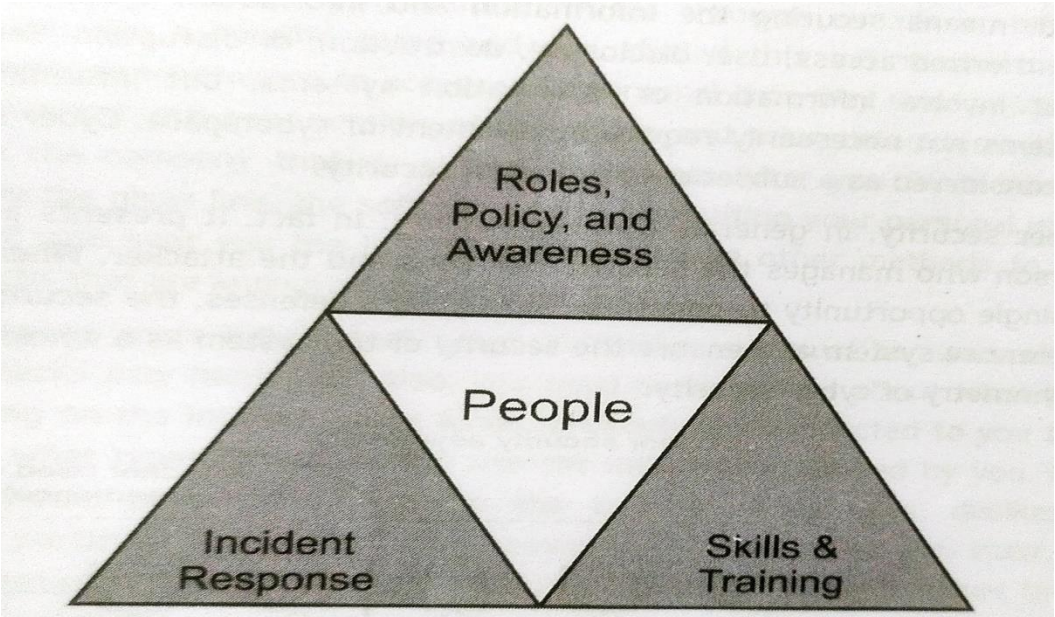


▲ Figure 13: Displaying the Scope of IA



▲ Figure 14: Showing Three-Dimensional IA Model

- Information States: Data in
  - Stored form
  - Processing form
  - Transmission form
- Security Services
  - Availability: Timely, reliable data to authorized users.
  - Integrity: Data in complete, accurate and consistent form, available to only authorized people.
  - Authentication: Validating the identity of individuals.
  - Confidentiality: Non disclosure of information.
  - Nonrepudiation: Non denial of action carried out.



▲ *Figure 15: Showing the Importance of People in IA*

b) Elaborate Security Risk Analysis. CO1 L1 7M

Security Risk Analysis

- System can be secure only at the depth of risk analysis.
- Analysis of risks is a process of identifying the threats, and measuring their effect on the security of the organization.
- Security involves assessment, analysis and management of risks.
- Assessment is identification of potential risk.
- Analysis is measuring the effects.
- Management of risks is steps in removing the vulnerabilities.
- See that the cost of security measures never exceed the possible losses.

- The common terminology:
  - Assets
  - Threats
  - Vulnerabilities
  - Countermeasures
  - Expected losses
  - Impact
- Risk analysis involve:
  - Impact statement
  - Effectiveness measure
  - Recommended countermeasure.

Unit -II

4. a) Write about data backup, archival. CO2 L3 7M

Data Backup

- Used against data loss due to accidents or malicious activities.
- Storage of **snapshot** of data at certain points.
- Take regular backups.
- Incase of loss of data, restore from latest backup.

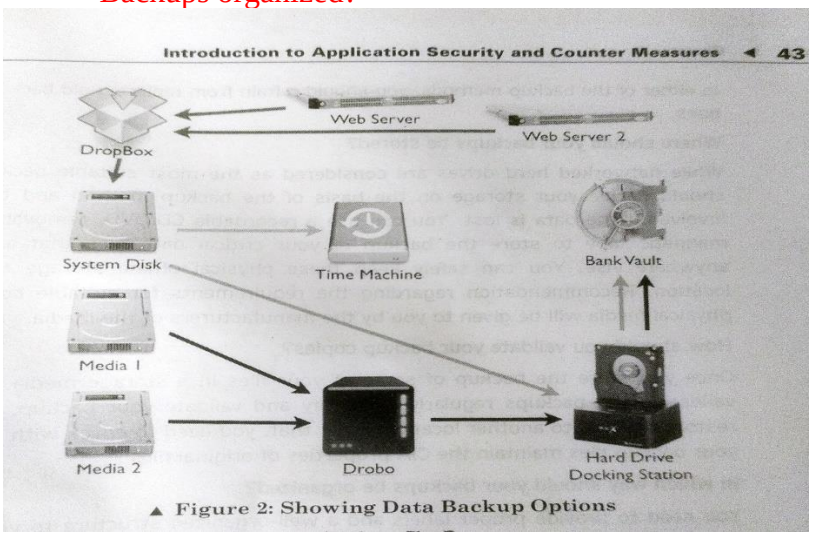
Data loss due to

- Failure of hardware.
- Fault in the media or s/w.
- Hacking/viruses.
- Power failure.
- Erroneous human activities. (deleting by mistake)

❑ Backup strategies should be based on quality of h/w and s/w, power supply, value of your data.

- Backup of entire system or few files?
- Any backup policy for the organization?
- Frequency of data backup?

- What storage media, for backup?
- In which format?
- Incremental or Differential backup?
- Where to store backups?
- How to validate backups?
- Backups organized?

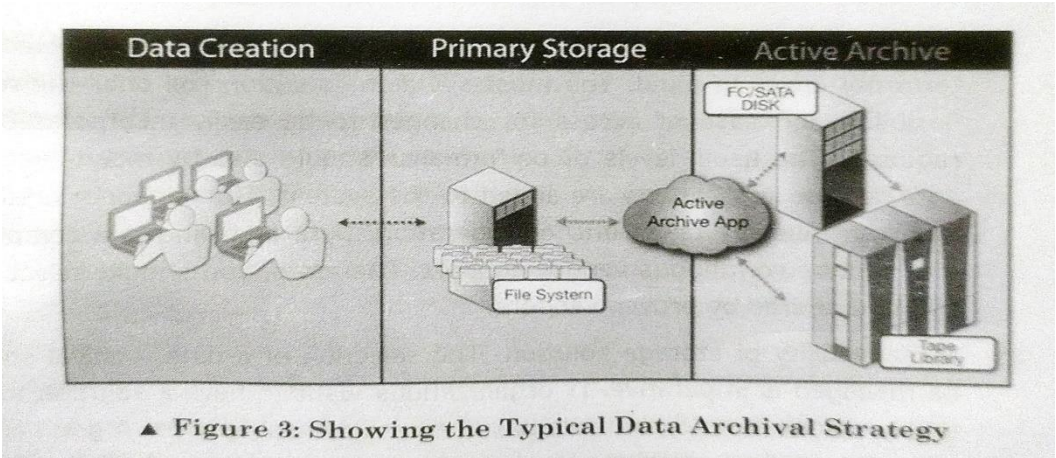


▲ Figure 2: Showing Data Backup Options

Data Archival

- Data is most valuable asset in an organization.
- Separation of non active data from actively used data is known as **archival.**
- Whenever old (archived) data is needed, it will be referenced.
- Obsolete data (not in active use) is archived.
- Archival is not same as data backup.
- Data is archived:

To reduce cost.
To save storage space in online system.
To reduce access complexity.
To improve system performance.



▲ Figure 3: Showing the Typical Data Archival Strategy

- Criteria for data archival has to be defined.
- Records being rarely changed or accessed and important but less accessed information are most suitable for archival.
- Archived data can also be used for historical researches.
- Archival solutions are chosen based on the following:
  - Longevity of storage solution.
  - Manageability of storage solution.
  - Amount of focus on intelligence of content.
  - Optimization of total cost of ownership.
  - Types of available solution.

b) Discuss about different threats to e-cash, credit/debit/smart cards and electronic payment CO2 L4 7M

system .

Security Threats to E-Commerce

- Each and every transaction on internet can be tracked, monitored, logged and stored.
- The threats may originate from internal or external sources.

Some of the top security threats:

- Unauthorized internal users accessing confidential information by using stolen passwords.
- Former employees, who have created alternative passwords, backdoors.
- Weak access points.
- Management that undermines security.
- Contractors, partners, consultants, competitors, etc…
- Businesses can make it mandatory to have firewalls, encryption, access policies for the organizations who ever deals with them.
- Growth of e-commerce necessitates maintaining privacy, security and safety in conducting online transactions.
- Initially, the mode of payment was cash, cheque, demand draft (DD).
- Now a days, it is e-cash and e-payment.

❑ **E-Cash**

- Electronic transfer of money in the form of a block of data representing money that is transferred online.
- Involves, computer networks, internet, and digitally stored value system.
- Contains a digital signature for authentication purposes.
- E-cash is generally stored on computers, or mobile devices in the form of software wallet programs.

E-Cash and Electronic Payment System

Describing the problems in E-Cash

- Double spending of money by a consumer.
- Double spending is the possibility of spending the token money, twice.
- Problem can be solved partly by providing unique serial number to e-cash.
- Seller can verify the serial numbers with the bank.
- E-cash may lead to money laundering(tax evasion, false accounting,..)

Maintaining E-Cash Privacy

- The bank and its customers need to keep the e-cash and its associated serial number, safe.
- The serial number (large enough) is selected by the customer randomly.
- Customer also can apply multiplier algorithm to the serial number and send a new number to the bank.
- Bank verifies this and assigns a private code to this number, sends back to the customer.

Avoiding double spending in E-Cash

- The bank has to maintain the records of serial numbers of all transactions.
- Requires non-editable software and cryptography algorithm for consumers details.
- Two part lock mechanism is used.
- One part is opened up with consumers identity.

The seller checks with the bank, after verification bank deposits the amount into sellers account

❑ **Electronic payment system**

Secure Electronic Payment Protocol/Secure Electronic Transaction (SEPP/SET)

- Open specification, uses digital signatures and user authentication.
- Developed by IBM, Cybercash, and MasterCard
- Used for bank card payments.
- SEPP messages are transmitted using Multipurpose Internet Mail Extensions (MIME).

Secure Courier Electronic Payment Scheme

- Encrypts data and authenticates the individual consumers and the buyers at the time of transactions.
- Many organizations such as Netscape, IBM, Open Market, GTE are working with Master Card.

CheckFree Wallet

- It is based on the client/server architecture, uses public-private key encryption technology.

- Uses RSA Rivest Shamir Adleman data security and large 768-bit key.
- Helps buyers and consumers to make transactions in easy and safe manner.
- Uses CyberCash, Netscape's SSL, VeriSign's digital ID for developing this system.

CyberCash

- Provides a secured mechanism to send the credit card information over the internet.
- Uses third party description for the transaction.

VeriSign

- Authenticates users by verifying the digital signatures.
- IBM introduced the concept of digital ID into its web browser and internet connection secure server.

DigiCash

- E-Cash based s/w that provides complete privacy.
- Used by Netherlands DigiCash NV.
- Credit card not required.
- Allows organizations to hold larger amounts of money.

Credit/Debit/Smart Cards

- Credit card is like postpaid card. Can spend, up to the limit.
- Debit card is like prepaid card. You need to have money in account to spend.
- Smart card contains an embedded microchip.
- Smart card can hold lot of information.
- More reliable and secure than credit or debit card.
- Smart card can perform tasks such as authentication, identification, data storage and application processing.
- Information security is, protection of information from illegal access or modification.

Privacy
Integrity
Authentication
Non-repudiation: Proof that information was indeed received.

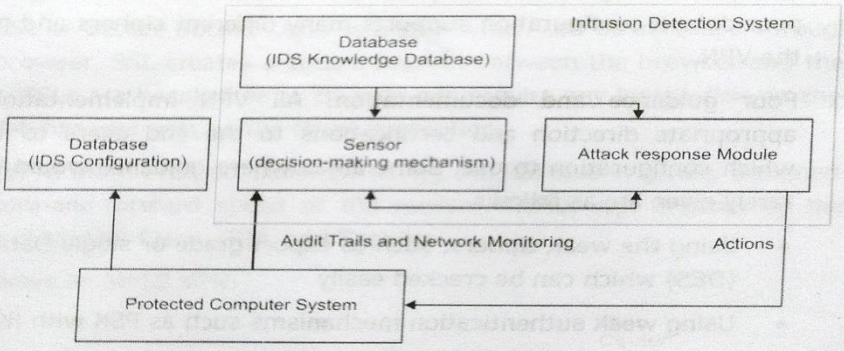
(OR)

5. a) Explain IDS, IDS components and types of IDS with diagrams. CO2 L1 7M

❑ **Intrusion Monitoring and Detection**

- The task of monitoring the network activities can be assigned to a computer or a set of computers.
- This system is kept on 24X7 with backup power.
- It keeps checking the computers with a ping command.
- The problems it can find are: overloaded systems, crashed servers, lost network connections, virus infections and power outages.
- Network administrator will be informed by a pager, phone call, email, …
- Regular virtual snapshots of network workflow are taken.
- The ID system generally tracks the user activities such as: web pages visited, sites, times,…
- The IDS will have a sensor which detects intrusions.

ıre 9 shows a sample IDS system:

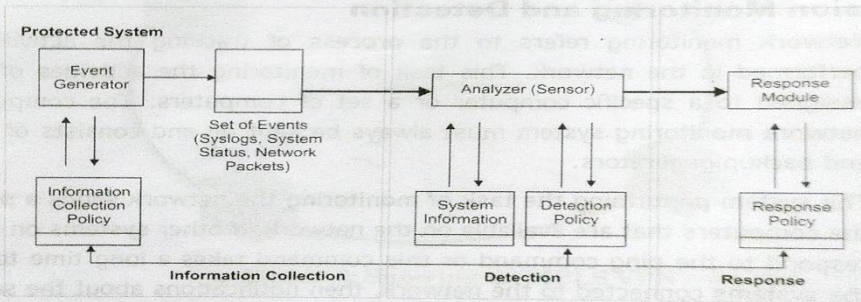


▲ **Figure 9: Showing a Sample IDS**

❑ **IDS Components**

▲ Figure 9: Showing a Sample IDS

Figure 10 shows the integration of different components with the sensor:



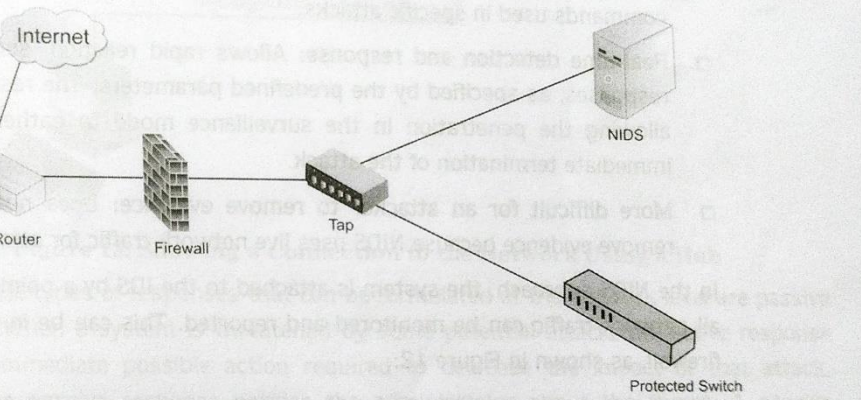
▲ Figure 10: Showing the IDS Components

- **Two types of IDS:**

1) **NIDS: Network based IDS**
2) **HIDS: Host based IDS**

NIDS

- Captures network traffic at specific points.
- Scans the network packets at the router or host level.
- Audits packet info and logs any suspicious packets.
- Scans its own database for attack signatures, then assign a severity level.
- Depending on the severity level informs the security team.
- Industries also employ scanners, sniffers, other network auditing and detection tools.

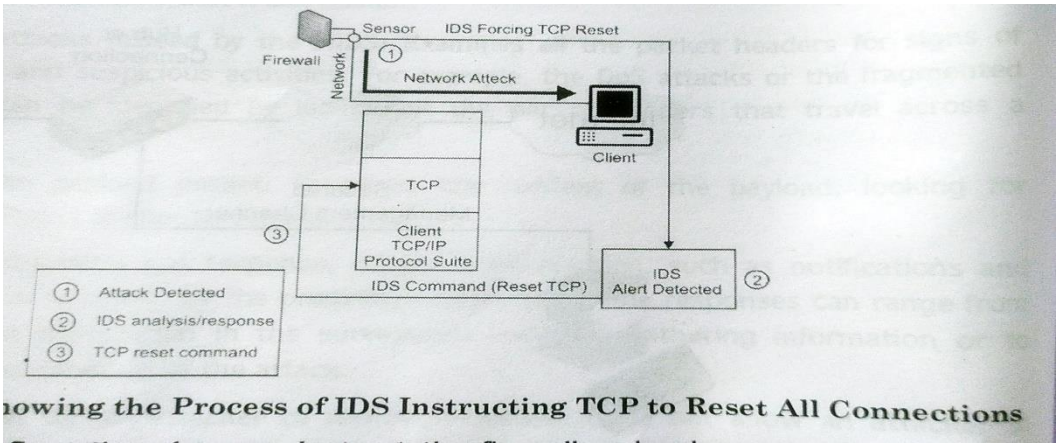


▲ Figure 11: Showing a Typical NIDS

- ❑ NIDS handles the following threats:
- IP spoofing
- Denial of service attacks
- DNS name corruption
- Man in the middle attacks

- ❑ Advantages of NIDS
- Lowers cost of ownership.
- Detects attacks missed by the HIDS
- Analyze the payload packet
- Real time detection and response

More difficult for an attacker to remove evidence.



owing the Process of IDS Instructing TCP to Reset All Connections

- **Host based IDS**
  - It is designed to monitor, detect, and respond to activities and **attacks on a given host**.
  - Monitors inbound as well as out bound.
  - HIDS are run on individual hosts or devices.
  - It checks various log files: kernel, system, server, network and firewall and compares with internal signature database for the attacks.
  - The data integrity of the important files and executables can be verified by HIDS.

HIDS may be incorporated in host's OS.

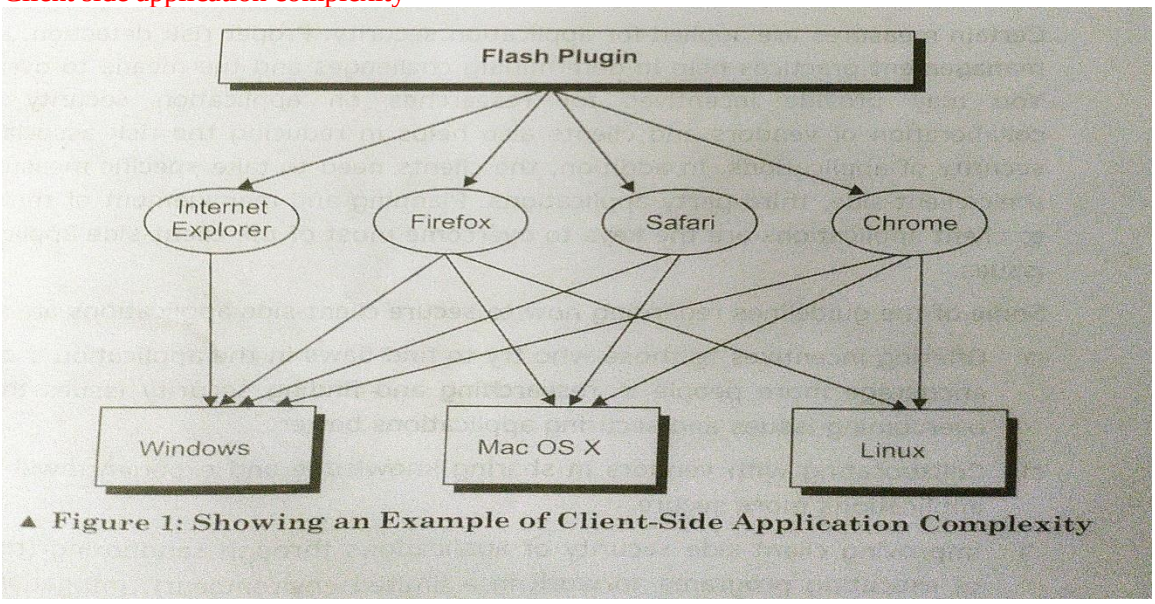
b) Write about Application Security. CO2 L3 7M

Application Security.

- To secure applications, firewalls, Virtual Private Networks VPNs, and access control systems, etc… are used.
- Attackers mostly target client side applications, browsers, multimedia programs, document readers, etc…
- Most of the OS vendors use patched systems to keep vulnerabilities to the minimum.

- **Vendor Challenges for Application Security**
  - Biggest challenge is various OS platforms, different versions of applications.
  - Compatible issues is another big issue.
  - Different platforms and versions have their own security considerations and requirements.

Client side application complexity



▲ Figure 1: Showing an Example of Client-Side Application Complexity

- **User Challenges for Application Security**
  - Vendors release patches in cycles.
  - System admins hardly care to download and install those patches.
  - Risk detection, analysis and management practices help.
  - Incentives for researchers on finding application security issues.

Guidelines

- Offering incentives to find flaws.

- Collaborating with vendors in sharing knowledge.
- **Sandboxing** client side security of applications (restricting rights of executing programs).
- Standardizing applications.

Updating s/w to newer versions.

Unit -III

6. a) Describe the application development security CO3 L4 7M

Application Development Security

- To avoid loss of information assets, organizations need secure application development strategy.

Primary issues are:

- Less trained/skilled developers.
- Less educational focus on secure development.
- Information not easily available.
- Security considered in last phases of lifecycles(not from the beginning).
- Compilers, interpreters not able to utilize system resources properly.
- Security measures are: antiviruses, IDS, firewalls, VPN, …
- Any vulnerability in the above will give away the data.
- So, secure applications have to be developed.

Common framework benefits

- Developers can refer to the common standards.
- Strict design principles and guidelines will help.
- Developers will follow security policy, language, tools.
- Better standards, procedures, security policy, methods.
- More objective view of the management.

Framework factors are Foundation, Principles, Design Guidelines

- **Foundation:** Basic knowledge of development procedure and security issues.
  - Security policy
  - Standards
  - Guidelines
  - Procedures
  - Development methodology
  - Preferred programming language
  - Compiler/Interpreter

Framework factors

- **Principles:** Basic rules to be followed during development.
  - Considering security as part of the design
  - Assuming hostile conditions
  - Using open standards
  - Restricted access
  - Authenticating users
  - Logging, monitoring, auditing
- **Design Guidelines:** Best code implementation methods.
  - **Validating Inputs:** Never trust input, always validate.
  - **Handling Exceptions:** Linked to security of applications in case of failures
  - **Applying Cryptography:** Provides confidentiality, integrity, availability and authentication.
  - **Using Random Numbers:** Computers generate pseudo random numbers, which can be predicted.

b) Explain about security governance and risk management. CO3 L2 7M

Information Security Governance and Risk Management

- Threats to information systems include purposeful attacks, environmental disruptions, human/machine errors,…

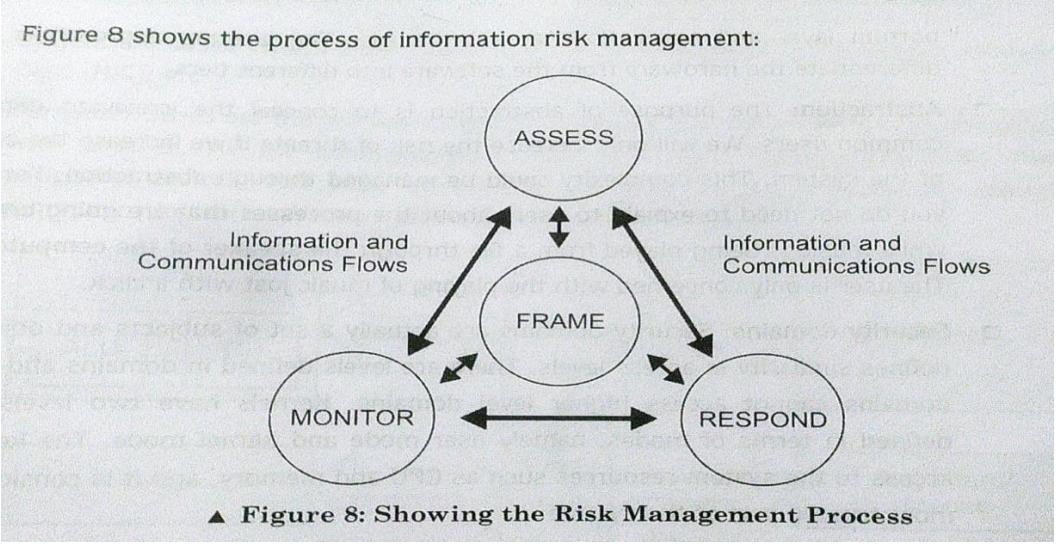
Key Elements

- Senior managers to manage risks.
- Executives recognizing the risks and their implications.
- Organization-wide risk tolerance level being established.
- Risk management programs being implemented.

4 activities of Risk Management

1. **Framing:** Sense a risk, act accordingly. Define certain actions, for different cases.

2. **Assessing:** Assess level of risk, level of damage.
3. **Monitoring:** Continuous check.
4. **Responding:** Taking preventive or corrective measures.



▲ **Figure 8: Showing the Risk Management Process**

(OR)

7. a) Discuss, what are the security issues related to hardware, data storage, and downloadable devices? CO3 L1 7M

Security Issues in Hardware, Data Storage, and Downloadable Devices

- Computer Systems include hardware, software, storage devices, OS, and peripheral devices.
- Each component has its own vulnerabilities.
- Security of every component of computer system is equally important, but issues of each of them are different.

❑ **Security Issues with Hardware**

- Hardware mainly faces security issues related to stealing, destruction, gaining unauthorized access and breaching the security code of conduct.

Ex: Laptops given to employees, they use it for illegitimate activities, which may lead to security threat.

Laptop damaged, data lost, etc..

Security mechanisms: Biometric access control, authentication tokens, Radio Frequency ID RFIDs, VPN, strong passwords, etc…

❑ **Security Issues with Storage Devices**

- Devices are: Compact Disks CDs, Digital Versatile Disk DVDs, memory cards, flash drives, …
- The threats to these devices can be external or internal.

Ex: data on a CD, unauthorized person have access to that CD.

- **Issues related to storage devices:** Loss, theft, disposal, stealing of data, denial of data, malware introduction, etc…
- Explaining the importance of security to individuals can improve and strengthen the security.
- Implement certain policies and procedures to provide all-round security to the storage devices and the data.

❑ **Security Issues with Downloadable (Peripheral) Devices**

Some of the devices are:

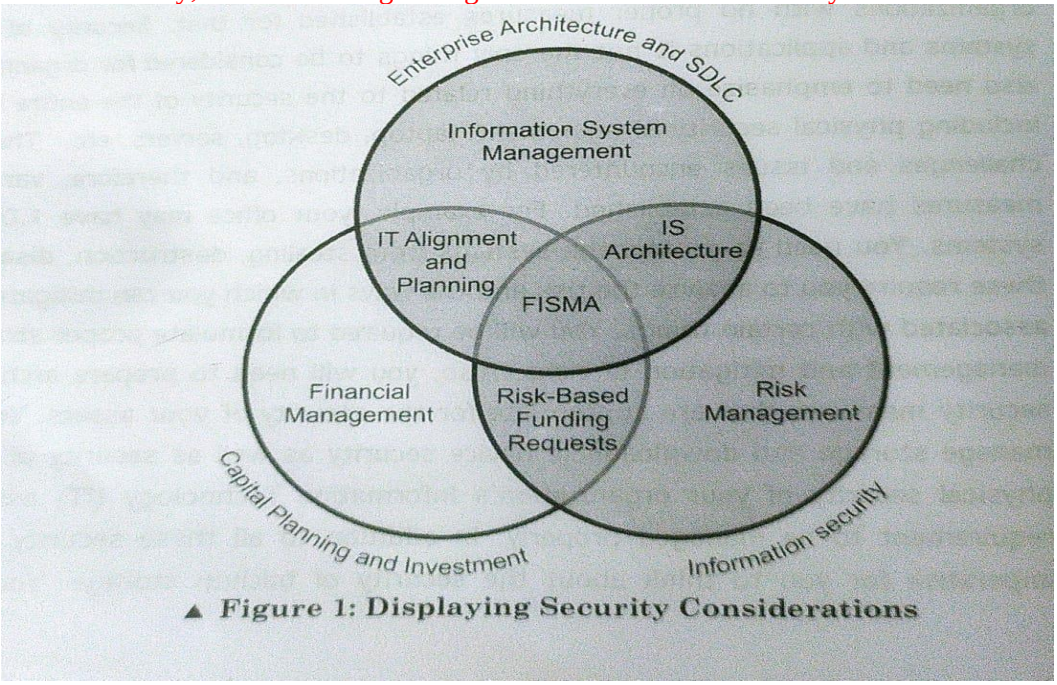
- Universal Serial Bus USB drives
- USB patch cards, that can be connected to a computer system.
- Electronic notebooks.
- Personal Digital Assistants PDAs.
- You can't easily detect threats to these devices, so more vulnerable.
- Protection of data from theft, manipulation or destruction.
- Protection of the devices from being stolen or destroyed.

b) Explain the process of developing secure information system, integrating with initial phase with a diagram. CO3 L2 7M

Secure Information System Development

- Security aspects, most crucial and challenging aspects for organizations, today.

- Protect the systems from stealing, destructions, disasters,…
- Need to formulate proper strategies for management and mitigation of risks.
- Have proper architecture for all security measures.
- Take care of backup storage.
- Identification and planning followed by mitigation of risks.
- Find balance between protection of information & assets, costs incurred for security, and formulating strategies for round the clock security.



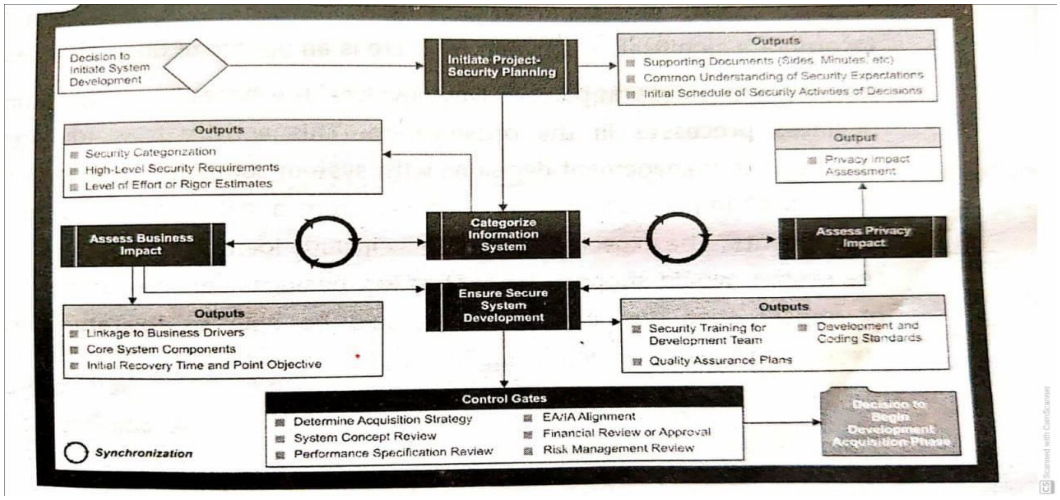
▲ Figure 1: Displaying Security Considerations

- SDLC has 5 phases

1. Initial Phase: size, complexity, schedule are analyzed.
2. Development Phase: System design and coding done.
3. Implementation Phase: Modules are tested and deployed.
4. Maintenance phase: Flaws in the system corrected, users feedbacks are taken, changes based on users requirements done.
5. Disposal Phase: Legacy systems are replaced by fresh, reengineered systems.

- Security has an important role in each phase of SDLC. The activities are:

Description: Represented as rectangular box as steps.
Output: Marked as Outputs.
Synchronization: R epresented by arrowed circles.
Interdependencies: Represented by arrows connecting boxes, loops.



Unit -IV

8. a) Explain semiconductor layout and design, in detail. CO4 L1 7M

to Semiconductor Layout and Design

- IC layout design is protected by SICLD
- SICLD – Semiconductor Integrated Circuits Layout Design Act 2000

Main features of SICLD

- Applicable to whole of India

- Registration with SICLD must for IPR protection.
- Defines the duration of validity
- Lists the IPR rights
- Specifies how infringement occurs
- Gives procedures for transferring, assignment of registered designs
- Specifies how the royalties are handled
- Gives steps to be taken in case of emergency
- Specifies penalties in case of:
  - Infringement
  - False claim of registration
  - Improperly describing a place of business
  - Falsification of entries in registration
  - Forfeiture of goods
  - Offences by companies
- Guidelines for agents
- Reciprocity with other countries

Steps involved in the layout registration

- Creator of the design needs to fill an application with SICLD Registry.
- The application may be accepted/accepted partially/rejected.
- Accepted ones are advertised within 14 days, 3 months wait period given for filing oppositions.
- Incase of opposition, counter has to be filed with in 2 months.
- Accept/Reject at the Registrar discretion.
- Aggrieved party can appeal for Appellate board or civil court.

b) Illustrate Various Security Policies and Their Review Process CO4 L3 7M

- The WWW policy
- The e-mail security policy
- The corporate policy

❑ **The WWW policy**

- The www is the universe of the internet accessible information.

The risks involved while browsing are:

- The s/w provided to the employee can be used for-profit outside business activity.
- s/w or documents downloaded may contain viruses.
- Employees can browse offensive material.

To avoid such risks while using www, a **WWW Policy** can be used

- No offensive or harassing material may be made available.
- No personal commercial advertising allowed.
- The personal material should be minimal.
- Company confidential material should not be made available.
- Users should not be permitted to install or run web servers.

❑ **E-mail Security Policy**

E-mails can be used

- For communication
- To transmit property information
- To harass others
- To engage in illegal activities
- To serve as evidence against the organization

10 commandments of E-mail security policy

1. Demonstrate the same respect thy gives to verbal communications.
2. Check thy spelling , thy grammar and read thrice before thou sent it.
3. Not to forward any chain letter.
4. Not transmit unsolicited mass e-mail to anyone.
5. Not send any hateful, harassing, threatening message to fellow users.
6. Not send any message that supports illegal or unethical activities.
7. Not to use to transmit sensitive info.
8. Not to use broadcasting except for appropriate announcements.
9. Keep thy personal usage to minimum.
10. Keep the policies and procedures sacred and help administrators protect them.

❑ **Corporate Policy**

- Formal declaration of principles and procedures of the company.

Contains:

- Company's mission statement
- Company's objectives
- Principles on the basis of which strategic decisions are made

Factors for measuring performance and ensuring accountability at all levels

- **Sample Security Policy**

Template

1. **Information Security Policy**
    a) Purpose
    b) Aims and commitments
    c) Responsibilities
    d) Councils
    e) Heads of departments
    f) Users and external parties
2. **Risk assessment and classification of information**
    a) Risk assessment of information
    b) Personal data

Protection of information systems and assets

4. Protection of confidential information

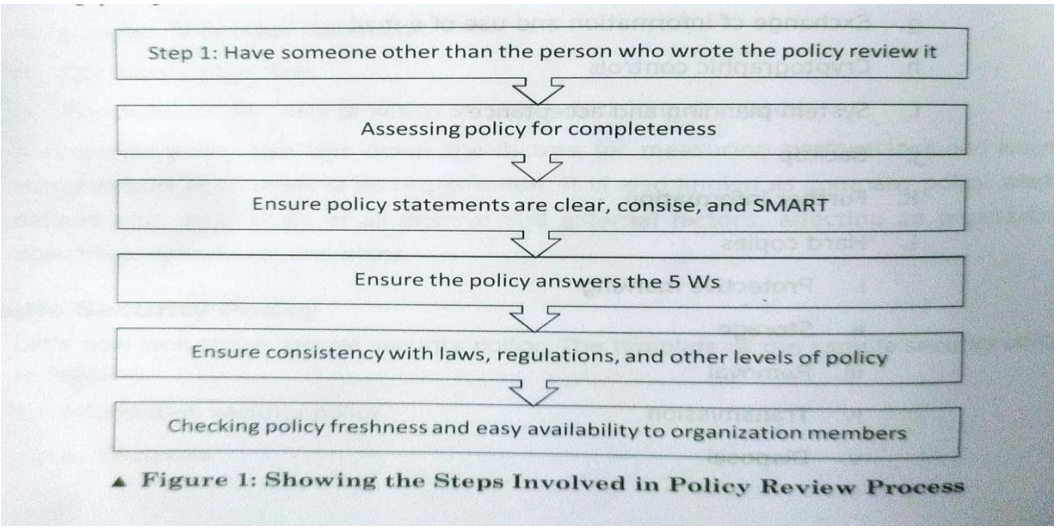
a) Storage
b) Access
c) Remote access
d) Copying
e) Disposal
f) Use of portable devices or media
g) Exchange of information and use of e-mail
h) Cryptographic controls
i) System planning and acceptance
j) Backup
k) Further information
l) Hard copies
    i. Protective marking
    ii. Storage
    iii. Removal
    iv. Transmission
    v. Disposal
m) Enforcement
n) Compliance
o) Other relevant policies or guidance
p) Contacts for further information
q) Sample risk assessment
r) Scope, criteria and organization
    i. Scope
    ii. Criteria

5. Risk identification and analysis

a) Assets
b) Threats and risks

6. Appendix 1: Sample risk assessment

7. Glossary



▲ Figure 1: Showing the Steps Involved in Policy Review Process

- **Policy Review Process**

Step 1: To be reviewed by someone other than the one who wrote
- The policy reviewer should be aware of the organization
- Technically sound

Step 2: Assessing policy for completeness
- Checks the existence of standards
- Checks if the policy is not flawed

Step 3: Ensuring the policy statements are clear, concise, SMART
- Simple and easily understandable.
- **SMART** stands for Specific, Measurable, Achievable, Realistic and Timebound

Step 4: Ensure the policy answer the 5 W s
- Who, What, When, Where, Why
- Policy should explain the purpose, background.

Step 5: Ensure consistency with laws, regulations and other levels of policy
- Else, may face with lawsuits.
- Country/state dependent

Step 6: Checking policy freshness and easy availability to members
- Keep it updated.

(OR)

9. a) Explain the ISO standards to be considered while laying down the policies. CO4 L2 7M

- **ISO/IEC 27002:2005 (Code of practice for information security management):**

Standards and Guidelines for Security Domains
- Security Policy
- Organization for information security
- Asset management
- Human resource security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management and compliance

- **ISO/IEC 27001:2005 (Information security management system ISMS – requirements):**

- Specifies the requirements for ISMS
  - Establishing
  - Implementing
  - Operating
  - Monitoring
  - Reviewing
  - Maintaining
  - Improving
- The standard defines a cyclic model Plan-Do-Check-Act PDCA.
- The phases of PDCA are:
  - The ‘plan’ phase to establish ISMS.

- The 'do' phase to implement ISMS.
- The 'check' phase to monitor and review ISMS.
- The 'act' phase to maintain and improve ISMS.

❑ **ISO/IEC 15408 (evaluation criteria for IT security)**

Helps an organization in evaluating, validating, and certifying the security assurance of a technology product.

❑ **ISO/IEC 13335 (IT security management)**

- ISO/IEC 13335-1:2004 Defines the concepts and models for information and communication technology security management.
- ISO/IEC TR 13335-3: 1998 Defines the techniques for the management of IT security.
- ISO/IEC 13335-4: 2000 Covers the selection of safeguards.
- ISO/IEC 13335-5: 2001 Covers management guidance on network security.

b) Explain Copyright act and patent law. CO4 L3 7M

Copyright

- Given in the fields of literature, dramatics, music, art, etc.
- Indian Copyright act 1976 gives the following rights:
  - To make copies of the work or to phonorecord (object with sound)
  - To prepare derivative works based on the original.
  - To distribute copies to the public by sale/rent/lease/lending
  - To perform the work in public
  - To display the work publicly
  - It is illegal for anyone to infringe any of the rights provided by copyright.

Work made for hire (employee/employer)

- Two general principles of copyright are:

1. Transfer of work to a person does not transfer the copyright with it.
2. Minor may claim copyright.

Copyrightable works:

1. Literary
2. Musical works
3. Dramatic works
4. Pantomimes (fairy tales) and choreographic works
5. Pictorial, graphic, and sculptural works
6. Motion picture
7. Sound recordings
8. Architectural works

Material not eligible for Copyright

- Works not in a tangible form of expression
- Titles, names, short phrases, slogans, familiar symbols or designs, lettering, coloring
- Ideas, procedures, methods, systems, concepts, principles,…
- Works that contain no original authorship

Ex: Standard calendars, height and weight charts

- Copyright is secured automatically upon creation.
- Phonorecords are material objects which contain fixations of sounds such as cassette tapes, CDs, …
- Publication is distribution of copies or phonorecords of a work to the public by sale or by other means.

Copyright Registration advantages

- Establishes a public record of the copyright claim.
- Registration is necessary before filing a case in a court.
- Supports the validity of a copyright.
- More useful if done with in three months of publication.

Can register with US Customs Service.

Patent

- A patent is a monopoly right granted by the state to an inventor.
- i.e. To make, use, license or sell an invention to the exclusion of others.
- Once the term of patent expires, the invention comes into the public domain.
- In India, patents are granted for 20 years.
- **The main objective of granting patents is to accelerate the technological and industrial development.**

- The patent ensures just reward to the inventor in terms of money and recognition.
- For the society, newer and better products, higher productivity leading to development, growth and prosperity.
- The number of patents filed and granted in a country is an indication of country's progress.
- There is no mechanism to obtain global patent, as patents are issued by the country.
- WIPO – World Intellectual Property Organization

PCT – Patent Cooperation Treaty, under this patent in multiple countries can be applied.

- **The Patent System**
- Granting monopolies to patents can be traced back to 600 years.
- It was a grant given by the King or the Queen to individuals, mainly for inventions.
- Indian Patent Act 1970, amended in 1999, 2002.
- **Patentable Invention**
- Defined as: A new product or process involving an inventive step and capable of industrial application.
- Invention must fulfill 3 requirements
- Invention must be '**new**'
- The invention must involve an **'inventive step'**

The invention must have **'industrial application'**

- **Nonpatentable Invention**
- A patent that can't be patented.

The categories which can't be patented:

- Which is detrimental to public order, morality, environment, or health
  - Ex: A new type of gambling machine
- An invention related to atomic energy. In India, it is purely central government area.
- Against the laws of nature, an abstract theory
- Discovery of living thing/non living substance or object
- A substance obtained by a mere mixture of certain components
- Arrangements or re-arrangement or duplication of known devices
- Traditional knowledge
- A mathematical or business method or a computer program or algorithms

- A method related to agriculture or horticulture.
- Any process related to the medicinal, surgical, curative, diagnostic, or other treatment of human beings and animals.
- Plants and animals in whole or part, excluding micro-organisms.
- Seeds and biological processes for the production of plants and animals.
- Literary, dramatic, musical or art are covered under Copyright act.
- A thin line exists between discovery and invention in biotechnology.
- USA didn't give patent for cloned sheep Dolly(ethical and legal issues)
- **Procedure for obtaining Patent**
- Can be applied by the true and first inventor or legal representative of a deceased person.

If the inventor is an employee of an organization, patent on employee name, ownership depending on the contract between employee and organization.