5.Information Security components:

- ✓ Confidentiality
- ✓ Integrity
- ✓ Availability(CIA)

IS is defined as “a state of well information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable”.

When we discuss data and information, we must consider the CIA triad. The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security.

CIA Triangle

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a morecomprehensive list of **critical characteristics** of information. At the heart of the study of informationsecurity is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.

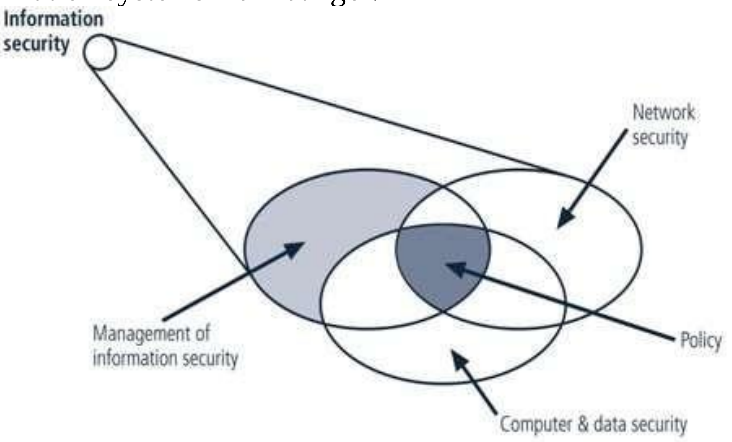

Figure 1.2.1.1 Components of Information Security

Confidentiality

Confidentiality of information ensures that only those with sufficient privileges may accesscertain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- ✓ Information classification
- ✓ Secure document storage
- ✓ Application of general security policies
- ✓ Education of information custodians and end usersExample, a credit card transaction on the Internet.
- ✓ The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, logfiles, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
- ✓ Giving out confidential information over the telephone is a breach of confidentialityif the caller is not authorized to have the information, it could result

in a breach of confidentiality.

Integrity

Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.

✓ Integrity means that data cannot be modified without authorization.

✓ Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast avery large number of votes in an online poll, and so on.

Availability

Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be eithera person or another computer system. Availability does not imply that the information is accessibleto any user; rather, it means availability to authorized users.

✓ For any information system to serve its purpose, the information must be available when itis needed.

✓ Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

6.THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

SDLC Waterfall Methodology

SDLC-is a methodology for the design and implementation of an information system in anorganization.

□ A methodology is a formal approach to solving a problem based on a structured sequenceof procedures.

□ SDLC consists of 6 phases.

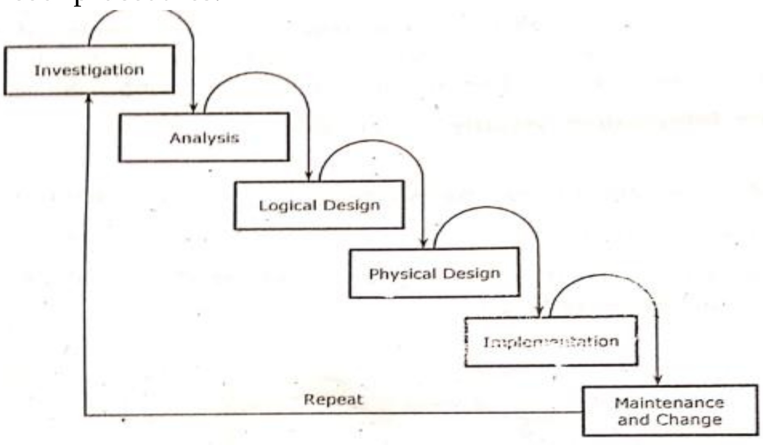

Figure 1.8.1 Systems Development Life Cycle

Investigation

- It is the most important phase and it begins with an examination of the event or plan thatinitiates the process.
- During this phase, the objectives, constraints, and scope of the project are specified.
- At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

- It begins with the information gained during the investigation phase.
- It consists of assessments (quality) of the organization, the status of current systems, andthe capability to support the proposed systems.
- Analysts begin by determining what the new system is expected to do, and how it willinteract with existing systems.
- This phase ends with the documentation of the findings and an update of the feasibilityanalysis.

Logical Design

- In this phase, the information gained from the analysis phase is used to begin creating asystems solution for a business problem.
- Based on the business need, applications are selected that are capable of providing neededservices.
- Based on the applications needed, data support and structures capable of providing theneeded inputs are then chosen.
- In this phase, analysts generate a number of alternative solutions, each withcorresponding strengths and weaknesses, and costs and benefits.
- At the end of this phase, another feasibility analysis is performed.

Physical design

- In this phase, specific technologies are selected to support the solutions developed in thelogical design.
- The selected components are evaluated based on a make-or-buy decision.

- ✓ Final design integrate various components and technologies.

Implementation

- ✓ In this phase, any needed software is created.
- ✓ Components are ordered, received and tested.
- ✓ Afterwards, users are trained and supporting documentation created.
- ✓ Once all the components are tested individually, they are installed and tested as asystem.
- ✓ Again a feasibility analysis is prepared, and the sponsors are then presented with thesystem for a performance review and acceptance test.

Maintenance and change

- ✓ It is the longest and most expensive phase of the process.
- ✓ It consists of the tasks necessary to support and modify the system for the remainder ofits useful life cycle.
- ✓ Periodically, the system is tested for compliance, with business needs.
- ✓ Upgrades, updates, and patches are managed.
- ✓ As the needs of the organization change, the systems that support the organization mustalso change.
- ✓ When a current system can no longer support the organization, the project is terminatedand a new project is implemented.

7.Laws and Ethics in Information security

As individuals we elect to trade some aspects of personal freedom for social order.

Laws are rules adopted for determining expected behavior in modern society and are drawn from Ethics,which define socially acceptable behaviors.

Ethics in turn are based on cultural mores: fixed moral attitudes or customs of a particular group. Some ethicsare recognized as universal among cultures.

Types of Law

• Civil law represents a wide variety of laws that are recorded in volumes of legal "code" available for reviewby the average citizen.

• Criminal law addresses violations harmful to society and is actively enforced through prosecution by thestate.

• Tort law allows individuals to seek recourse against others in the event of personal, physical, or financialinjury.

• Private law regulates the relationship between the individual and the organization, and encompasses familylaw, commercial law, and labor law.

• Public law regulates the structure and administration of government agencies and their relationships withcitizens, employees, and other governments, providing careful checks and balances. Examples of public law include criminal, administrative, and constitutional law.

Relevant U.S. Laws – General

Computer Fraud and Abuse Act of 1986

National Information Infrastructure Protection Act of 1996USA
Patriot Act of 2001

Telecommunications Deregulation and Competition Act of 1996
Communications Decency Act (CDA)

Computer Security Act of 1987

Privacy

The issue of privacy has become one of the hottest topics in information

The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up

The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities

Privacy of Customer Information

Privacy of Customer Information Section of Common Carrier Regulations
Federal Privacy Act of 1974

The Electronic Communications Privacy Act of 1986

The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known asthe Kennedy-Kassebaum Act

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999

13. Ethics and policies applied in IS

Cultural Differences in Ethical Concepts
□Differences in cultures cause problems in determining what is ethical and what is not ethical

□Studies of ethical sensitivity to computer use reveal different nationalities have different perspectives

□Difficulties arise when one nationality's ethical behavior contradicts that of another national group

Ethics and Education Employees must be trained and kept aware of a number of topics related to information security, not the least of which is the expected behaviors of an ethical employee

✓This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal

✓Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user Deterrence to Unethical and Illegal Behavior

✓Deterrence - preventing an illegal or unethical activity

Risk Management
Inventorying Assets
Risk Assessment is the documented result of the risk identification process
Identifying Threats &Vulnerabilities
Risk Control
Selecting Strategy
Classifying Assets

✓Laws, policies, and technical controls are all examples of deterrents

✓Laws and policies only deter if three conditions are present:
Fear of penalty
Probability of being caught
Probability of penalty being administered

8.RISK IDENTIFICATION

IT professionals to know their organization's information assets through identifying,classifying and prioritizing them.

Assets are the targets of various threats and threat agents, and the goal is to protect theassets from the threats.

Once the organizational assets have been identified, a threat identification process isundertaken.

The circumstances and settings of each information asset are examined to identifyvulnerabilities.

When vulnerabilities are found, controls are identified and assessed as to their capabilityto limit possible losses in the eventuality of attack.

The process of Risk Identification begins with the identification of the organization'sinformation assets and an assessment of their value.

TheComponents of this process are shown in figure.

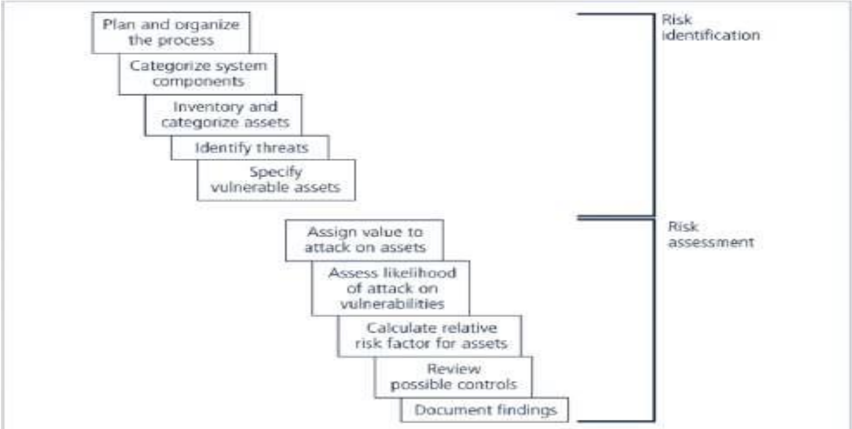
Plan and organize the process
Categorize system components
Inventory and categorize assets
Identify threats
Specify vulnerable assets
Risk identification
Assign value to attack on assets
Assess likelihood of attack on vulnerabilities
Calculate relative risk factor for assets
Review possible controls
Document findings
Risk assessment

Figure 2.3.1 Components of Risk Identification

Asset Identification & Valuation Includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements. Then, you classify and categorize the assets, adding details.

RISK ASSESSMENT

Assigns a risk rating or score to each Information asset.
It is useful in gauging the relative risk to each Vulnerable asset.

Valuation of Information assets

Assign weighted scores for the value to the organization of each Information asset.National Institute of Standards & Technology (NIST) gives some standards.
To be effective, the values must be assigned by asking he following questions. Which threats present a danger to an organization's assets in the given environment? Which threats represent the most danger to the organization's Information?
How much would it cost to recover from a successful attack?
Which of the threats would require the greatest expenditure to prevent?

Likelihood

It is the probability of specific vulnerability within an organization will be successfully attacked.
NIST gives some standards.
0.1 = Low 1.0 = High
Eg: Number of network attacks can be forecast based on how many network address the organization has assigned.

Risk Determination

Risk = [(Likelihood of vulnerability occurrence) X (Value of information Asset)]____(% of risk mitigatedby current controls) + uncertainty of current knowledge of the Vulnerability

For the purpose of relative risk assessment, risk equals:
Likelihood of vulnerability occurrence TIMES value (or impact) MINUS percentage risk already controlled PLUS an element of uncertainty

Eg: Information Asset A has a value score of 50 & has one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

Solution:

Risk = [(1.0) x 50] – 0 % + 10%
= (50 x 1.0) – ((50 x 1.0)x 0.0) + ((50 x 1.0) x 0.1)
= 50 – 0 + 5
= 55

Identify Possible Controls (For Residual Risk)

Residual risk is the risk that remains to the information asset even after the existing control has beenapplied.
Three general categories of controls

1. Policies
2. Programs
3. Technologies

1. Policies

   General Security
   Policy Program
   Security PolicyIssue
   Specific Policy
   Systems Specific
   Policy

2. Programs
   Education
   Training
   Awareness
3. Security Technologies

Technical Implementation Policies

Access Controls

Specially addresses admission of a user into a trusted area of the organization.Eg: Computer rooms, Power Rooms.
Combination of policies , Programs, & Technologies

Types of Access controls

Mandatory Access Controls (MACs)

- Give users and data owners limited control over access to information resources.

Nondiscretionary Controls

- Managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Discretionary Access Controls (DAC)

- Implemented at discretion or option of the data userLattice-based Access Control
- Variation of MAC - users are assigned matrix of authorizations for particular areas of access.

Documenting the Results of Risk Assessment

By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them.

The goal of this process is to identify the information assets that have specific vulnerabilities and listthem, ranked according to those most needing protection. You should also have collected some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown in the following table.

Table 2.4.5.1 Ranked vulnerability risk worksheet

Asset	Asset Impact or Relative value	Vulnerability	Vulnerability Likelihood	Risk Rating Factor
Customer Service Requestvia e-mail(inbound)	55	E-mail disruption due to hardware Failure	0.2	11
Customer order via SSL - (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL - (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer Service Requestvia e-mail(inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer Service Requestvia e-mail(inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL - (inbound)	100	Lost orders due to Web server denialof-service attack	0.025	2.5
Customer order via SSL (inbound)SSL-Secure Sockets Layer	100	Lost orders due to Web server software Failure	0.01	1

RISK CONTROL STRATEGIES

Four basic strategies to control each of the risks that result from these vulnerabilities.

1. Apply safeguards that eliminate the remaining uncontrolled risks for the vulnerability [Avoidance]
2. Transfer the risk to other areas (or) to outside entities[transference]
3. Reduce the impact should the vulnerability be exploited[Mitigation]
4. Understand the consequences and accept the risk without controlor mitigation[Acceptance]

Avoidance

It is the risk control strategy that attempts to prevent the exploitation of the vulnerability, and isaccomplished by means of

1. Countering threats
2. Removing Vulnerabilities in assets
3. Limiting access to assets 4. Adding protective safeguards.Three common methods of risk avoidance are

1. Application of policy
2. Application of Training & Education
3. Application of Technology

Transference

Transference is the control approach that attempts to shift the risk to other assets, other processes, orother organizations.

It may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing Insurance, Implementing Service contracts with providers.

Top 10 Information Security mistakes made by individuals.

1. Passwords on Post-it-Notes
2. Leaving unattended computers on.

1. Opening e-mail attachments from strangers.
2. Poor Password etiquette
3. Laptops on the loose (unsecured laptops that are easily stolen)
4. Blabber mouths (People who talk about passwords)
5. Plug & Play[Technology that enables hardware devices to be installed and configured without the protection provided by people who perform installations] 8. Unreported SecurityViolations

9. Always behind the times.
10. Not watching for dangers inside the organization

Mitigation

It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning & preparation.

Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently and effectively. Includes 3 types of plans.

1. Incident response plan (IRP) -Actions to take while incident is in progress
2. Disaster recovery plan (DRP) - Most common mitigation procedure.
3. Business continuity plan (BCP) - Continuation of business activities if catastrophic event occurs.

1. Incident Response Plan (IRP)

This IRP Plan provides answers to questions such as

1. What do I do now?
2. What should the administrator do first?
3. Whom should they contact?
4. What should they document?

2.The IRP Supplies answers.

For example, a system's administrator may notice that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee.

The IRP also enables the organization to take coordinated action that is either predefined and specificor ad hoc and reactive.

3.Disaster Recovery Plan (DRP)

Can include strategies to limit losses before and during the disaster.

Include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the floodwater recede.

DRP focuses more on preparations completed before and actions taken after the incident, whereas theIRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent,concrete actions.

4.Business Continuity Plan (BCP)

BCP is the most strategic and long term of the three plans.

It encompasses the continuation of business activities if a catastrophic event occurs, such as the lossof an entire database, building or operations center.

The BCP includes planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.

Many companies offer this service as a contingency against disastrous events such as fires. Floods, earthquakes, and most natural disasters.

Acceptance

It is the choice to do nothing to protect a vulnerability and do accept the outcome of its exploitation. This strategy occurs when the organization has:

- Determined the level of risk.
- Assessed the probability of attack.
- Estimated the potential damage that could occur from attacks.
- Performed a thorough cost benefit analysis.
- Evaluated controls using each appropriate type of feasibility.
- Decided that the particular function, service, information, or asset did not justify the costof protection.

Selecting a Risk Control Strategy

Level of threat and value of asset play major role in selection of strategy Rules of thumb on strategy selection can be applied:

- When vulnerability (flaw or weakness) exists: Implement security controls to reduce thelikelihood of a vulnerability being exercised.
- When vulnerability can be exploited: Apply layered protections, architectural designs, andadministrative controls to minimize the risk.
- When the attacker's cost is less than his potential gain: Apply protections to increase theattacker's cost.
- When potential loss is substantial: Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss.

11.CRITICAL CHARACTERISTICS OF INFORMATION

CRITICAL CHARACTERISTICS OF INFORMATION

- ✓ Confidentiality
  - ▪ Integrity
- ✓ Availability
  - ▪ Privacy
  - ▪ Identification
  - ▪ Authentication
  - ▪ Authorization
  - ▪ Accountability
- ✓ Accuracy

Confidentiality

Confidentiality of information ensures that only those with sufficient privileges may accesscertain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- ✓ Information classification
- ✓ Secure document storage
- ✓ Application of general security policies

- ✓ The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, logfiles, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
- ✓ Giving out confidential information over the telephone is a breach of confidentialityif the caller is not authorized to have the information, it could result in a breach of confidentiality.

Integrity

Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.

- ✓ Integrity means that data cannot be modified without authorization.
- ✓ Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast avery large number of votes in an online poll, and so on.

Availability

Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be eithera person or another computer system. Availability does not imply that the information is accessibleto any user; rather, it means availability to authorized users.

- ✓ For any information system to serve its purpose, the information must be available when itis needed.
- ✓ Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Privacy

The information that is collected, used, and stored by an organization is to be used only forthe purposes stated to the data owner at the time it was collected. This definition of privacy does focus on freedom from observation (the meaning usually associated with the word), but rather means that information will be used only in ways known to the person providing it.

Identification

An information system possesses the characteristic of identification when it is able to recognize individual users. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.

Authentication

Authentication occurs when a control provides proof that a user possesses the identity thathe or she claims.

- ✓ In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents(electronic or physical) are genuine(i.e. they have not been forged or fabricated)

Authorization

After the identity of a user is authenticated, a process called authorization provides assurance that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.