Application Development Security Issue:-

8.1 INTRODUCTION

Developing secure information systems requires addressing a number of issues in data security, network security and physical security.

Data Security

- What access controls, integrity controls, and backup procedures are in place to limit attacks?
- Are there privacy policies and procedures that users must comply to?
- What data access controls (authorization, authentication, and implementation) are there?
- What user responsibilities exist for management of data and applications?
- Have direct access storage device management techniques been defined? What is their impact on user file integrity?
- Are there procedures for handling sensitive data?

Network Security

- What kinds of access controls (Internet, wide area network connections, etc.) are in place?
- Are there authentication procedures? What authentication protocols are used for local area networks, wide area networks and dialup servers? Who has the responsibility for security administration?
- What type of network media, for example, cables, switches, and routers are used? What type of security do they have?

Scanned by CamScanner

- Is security implemented on file and print servers?
- Does the organization make use of encryption and cryptography for use over the Internet, Virtual Private Networks (VPNs), e-mail systems, and remote access?
- Does the organization conform to networking standards?

Physical Security

- Are there locks and entry procedures to gain access to servers?
- Is there sufficient air conditioning and are air filters being cleaned out regularly? Are air conditioning ducts safeguarded against break-ins?
- Are there uninterruptible power supplies and generators and are they being checked through maintenance procedures?
- Is there fire suppression and pumping equipment, and proper maintenance procedures for the equipment?
- Is there protection against hardware and software theft? Are software packages and licenses and backups kept in safes?
- Are there procedures for storing data, backups, and licensed software off-site and onsite?

We have already discussed issues concerning data security and network security. Physical security is discussed in detail in the next chapter. The concept of system development life cycle was introduced in chapter one. Here we begin with how the various security issues have to be decided during the system development life cycle of an information system.

6.2 APPLICATION DEVELOPMENT SECURITY

The system (application) development life cycle starts with the initiation of the system planning process, and continues through system acquisition and development, implementation, operations and maintenance, and ends with disposition of the system as shown in fig (1). Specific decisions about security must be made in each of these phases to assure that the application is secure.

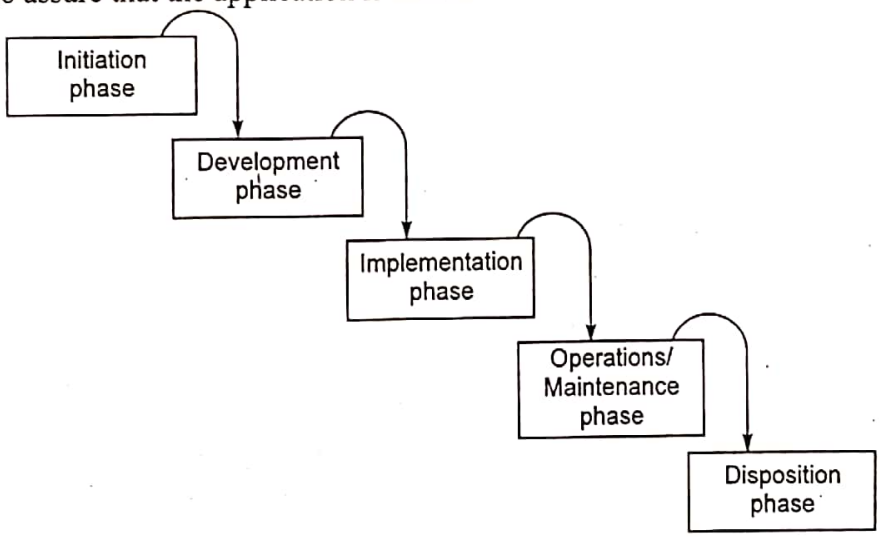

Fig. (1) Application development life-cycle

Scanned by CamScanner

[I] Initiation Phase

The initiation phase begins with a determination of need for the system. The organization develops its initial definition of the problem that could be solved through automation. This is followed by a preliminary concept for the basic system that is needed, a preliminary definition of requirements, and feasibility and technology assessments. Also during this early phase, the organization starts to define the security requirements for the planned system. Management approval of decisions reached is important at this stage.

The information developed in these early analyses will be used to estimate the costs for the entire life cycle of the system, including information system security. An investment analysis should be performed to determine the appropriate strategy for achieving the system requirements, while taking mission needs and budget constraints into account. Expenditures for security should be considered before the system is built. It is difficult to add functionality into a system after it has been built, and it is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on.

During this initiation phase, the organization establishes the security categorization and conducts a preliminary risk assessment for the planned information system. Categorization of the information system using standards and guidelines aids system security planners in defining information system security according to levels of impact, and in selecting a baseline of initial security controls for those impact levels. There are various levels of potential impact on organizations or on individuals should certain adverse events occur. These are events that could jeopardize the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are then used in conjunction with vulnerability and threat information to assess the risk that an organization faces.

A *preliminary risk assessment* should be performed to develop a brief initial description of the basic security needs of the system, including needs to protect the integrity, availability, and confidentiality of system information. The preliminary risk assessment should define the threat environment in which the system will operate and the potential vulnerabilities. This assessment should be followed by an initial identification of required security controls that will protect the system in its operational environment. A detailed risk assessment is developed in the next phase.

[II] Acquisition/Development Phase

In this phase, the organization should conduct a *requirements analysis*, which draws on and expands the work done in the Initiation phase. This in-depth study of the organization's need for the system should analyze the security aspects of the system requirements.

(1) A ***formal risk assessment*** identifies threats to and vulnerabilities in the information system, the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on assets or operations, and the security controls that are needed. This analysis builds on the initial risk

Scanned by CamScanner

assessment performed during the Initiation phase, but is more detailed and specific. The risk assessment brings together important information about the protection of the information system, and it generates information required for the security plan. This risk assessment should be conducted before the approval of design specifications. The assessment should consider existing controls and their effectiveness, as well as the impact that the new system might have on other systems to which it will be directly or indirectly connected. Enterprise security architectures can help to minimize the vulnerabilities that might be introduced by the new system.

(2) The ***security functional requirements analysis*** considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

(3) The ***security assurance requirements analysis*** addresses the activities and assurance needed to produce the desired level of confidence that the information security will work correctly and effectively. This analysis, based on legal and functional security requirements, should be used to determine how much and what kinds of assurance are required. The goal is to achieve cost-effective assurance that meets the requirements for protecting the organization's information assets. Tests and evaluations can provide information about system quality and support confidence in the system. Third-party and other evaluations can be used, but the objectivity of these evaluations must be considered. Government organizations may conduct their own evaluations. Other sources of evaluations include trade, professional, and commercial organizations.

(4) ***Consideration and reporting*** of development cost enable organizations to determine how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training. The best source of this data is the risk assessment, which identifies the controls that will mitigate vulnerabilities, and includes a cost-benefit analysis of recommended controls based on consideration of the possibility of an incident and its potential impact. When the controls have been selected, the cost of each can be determined.

(5) The ***security plan*** ensures that the planned or existing security controls are fully documented. The security plan also provides a complete description of the information system, and provides references to key documents supporting the organization's information security program : the configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behaviour, risk assessment, security test and evaluation plan, system interconnection agreements, security authorizations and accreditations, and the plan of action with milestones.

Scanned by CamScanner

(6) A study of ***security controls*** focuses on the controls described in the security plans to assure that they are designed, developed, and implemented. Additional controls may be needed for information systems currently in operation.

(7) A ***security test and evaluation plan*** should be developed for the security controls that can be evaluated prior to deployment. The controls must be tested and evaluated for correct implementation and effectiveness. Controls of a non-technical activity, such as management and operational controls, cannot be tested and evaluated until the information system is deployed.

(8) ***Other planning processes,*** studies, evaluations, and contract specifications associated with the development and acquisition process, involving appropriate staff members, help to assure that the security requirements of the system are identified and achieved. The IT security experts should work with the contracting office to select the most advantageous type of contract. A team or group of participants from functional areas such as legal, human resources, information security, and physical security can provide useful perspectives in reviewing the plans. Involvement of appropriate staff early in the planning process can help to reduce life-cycle costs and make it easier to change requirements early on.

[III] Implementation Phase

In this phase, the system is installed and evaluated in the organization's operational environment.

(1) ***Inspection and acceptance*** of the delivered system is necessary to verify that the functionality described in the specifications has been included in the deliverables. Testing can be done by the organization or by an independent contractor to assure that the system meets the specifications, and that the security features are operating.

(2) ***Security controls are integrated*** at the site where the system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

(3) The system should be ***certified and accredited*** before it is operational. *Security certification* gives organization officials confidence that the appropriate safeguards and countermeasures are in place. Security certification also uncovers and describes the known vulnerabilities in the information system. This information helps officials make decisions about *security accreditation,* which is an authorization for a system to operate. Granted by a senior organization official, accreditation is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an acceptance of identified residual risk to agency assets or operations. The decision is risk-based and is supported by testing and evaluation results produced during the security control verification process.

Scanned by CamScanner

[IV] Operations/Maintenance Phase

In this phase of the SDLC, information systems are operating, and may undergo enhancements and modifications. Hardware and software may be added or replaced. The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed to determine how it can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to the organization's changing needs.

(1) ***Configuration management and control*** procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently to controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant impact on the security of the system. System changes should be documented, and their potential impact on security should be assessed regularly.

(2) Controls must be ***continuously monitored*** through periodic testing and evaluation to assure that they are effective in their application. Monitoring of security controls verifies the continued effectiveness of those controls and reports on the security status of the system's information.

[V] Disposition Phase

This phase provides for disposal and/or contract closeout of the system (for contracts that were employed during the earlier phases). Disposal of the system may involve a separate contract. For some systems, there may not be a definitive end to the SDLC since the system may evolve or transition to the next generation of technology, as a result of changing requirements. System security plans should be modified to evolve with the system.

(1) ***Information should be retained*** to conform to current legal requirements and to accommodate future technology changes that might make the system's data retrieval method obsolete. The environmental, management, and operational information about a system may be relevant and useful in developing the security plan for the follow-on system. The data processed by the system should be preserved for use in a follow-on system or archived in accordance with applicable regulations and policies.

(2) Data should be deleted, erased, and written over as necessary, and the media that stored the data should be sanitized. Degaussing, overwriting, and media destruction are some of the methods that may be used.

(3) ***Disposal of the hardware and software*** should be completed at the direction of the information system security officer.

6.3 INFORMATION SECURITY GOVERNANCE

Governance collectively represents the system of policies, standards, guidelines and procedures that are needed for an organization's operation and decisions. Let us

Scanned by CamScanner

first discuss the various principles and concepts on which the information security governance is based.

6.3-1 CONCEPT AND PRINCIPLES IN INFORMATION SECURITY GOVERNANCE

(1) *CIA Triad* : We have already discussed the three concepts of information security often called the CIA triad as shown in fig. (2)

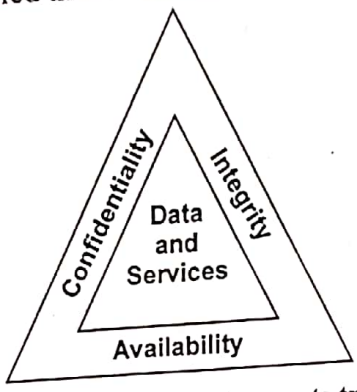

Fig. (2) Security requirements triad

- Balancing confidentiality, integrity and availability creates security in the information systems.
- Confidentiality issues concern with prevention of unauthorized use or disclosure of information.
- Integrity issues are concerned with accuracy and completeness of data such as :
  - Unauthorized users don't modify data.
  - Authorized users don't make unauthorized modifications (insider threat).
  - Data isn't damaged in processing or transit.
- Availability is concerned with issues regarding authorized users accessing the information system and accessing data as needed.
- Denial of Service attacks harm availability
- Other threats to availability are.
  - Single points of failure
  - Inadequate capacity planning
  - Malfunctions
  - Fail-safe controls
  - Disasters

(2) *Defence in depth* : There should be multiple layers of defence in the information systems.

- Various security management principles are applied for this purpose such as data classification, personnel security policies and practices, security awareness programs etc.
- Security technologies available are firewalls, IDS, antivirus and various access controls.
- Different vendors on different layers in the system also help in secured systems.

Scanned by CamScanner

(3) *Data Classification* :

- The classification of information is an important aspect of security governance.
- The same protection scheme created to prevent production data from accidental release to the wrong party should be applied to security policies in order to keep information freely available, but only within the organization.
- In today's open office environments, it may be beneficial to implement a clean desk policy. A clean desk policy stipulates that at the end of the business day, all classified information must be properly stored and secured.

(4) *Mission statements, goals and objectives* :

- Mission statement provides the reason for an organization's existence. It is also called philosophy or vision statement.
- An organization works to accomplish it goals and objectives.
- Good security governance requires that security concerns should be visible in mission statements, goals and objectives.

(5) *Policies, standards, guidelines and procedures* :

- *Security policies* are formal statement of rules.
- Security policies are of four types :
  - High-level policies—these come from senior management and define objectives, responsibilities, ethics, requirements and controls.
  - Regulatory
  - Advisory (most common type)
  - Informative
- *Standards* define and support higher-level policies. These are specific mandatory requirements which specify in detail what must be done to comply with policies. For example, standards can even specify exact brand, product or protocol to be used for developing secure IS.
- *Guidelines* are similar to standards. These are recommendations which are not compulsory.
- *Procedures* are instructions on how to implement policies and meet the criteria defined in standards.
- Policies, standards, guidelines and procedures all work together to :
  - establish governance
  - provide guidance and decision support
  - help establish legal authority

6.3-2 INFORMATION SECURITY GOVERNANCE PRACTICES

The various information security governance practices are :

(1) Third-Party Governance

- IT functions are often outsourced to :
  - Call-centres

Scanned by CamScanner

- Application development

- Outsourcing security issues are :
  - Access control (discussed in chapter 3)
  - Maintenance hooks (backdoors/trapdoors discussed in chapter 5)
  - Service-Level Agreements (SLAs)
- Service-Level Agreements (SLAs) establish minimum performance standards.
- Internal SLAs are concerned with agreements between one part of an organization to another.
- Outsourcing SLAs specify what vendors must provide for example,
  - 99.999% uptime
  - Help desk response time

(2) Identity Security Management

These govern issues such as :

- Account provisioning and de-provisioning
- Access control
- Directory services
- Public Key Infrastructure

(3) Personnel Security Polices and Practices

- Background checks and security clearances should be done on all employees. This includes verification of data in employee's application/resume, reference checks, credit records etc.
- Employment agreements should include the non-disclosure clause and acceptable company items use policy.
- Fair and uniform hiring and termination practices should be followed in the organisation.
- In case of termination/exit of an employee it should be ensured :
  - Surrender of keys, badges, phones, laptops etc.
  - Change locks and passwords and disable network accounts.
  - Notify customers, partners, vendors etc.

(4) Security Roles and Responsibilities

- Roles and responsibilities must be clearly defined in job descriptions. This reduces confusion and ambiguity.
- Also, it provides a legal basis for employee's authority or actions.
- In case of negligence of an employee, action can be initiated.

(5) Separation of Duties

- This ensures that no single individual has complete authority or control over a critical system or process.
- Reduces opportunity for waste, fraud, or abuse.

Scanned by CamScanner

- Two-man control reduces dependency on individuals (avoiding single points of failure).

(6) **Job Rotation**

- Transferring key personnel to other positions or departments is also important for security governance.
- This reduces opportunity for waste, fraud, and abuse.
- Also, it reduces dependence on individuals.
- It promotes professional growth.
- It reduces monotony and fatigue.

6.4 RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure confidentiality, integrity and availability of all the components in the organization's information systems. Hence, it is the formal process of identifying and controlling the risks facing an organization. In other words, it can also be defined as the probability of an undesired event causing damage to an asset.

To keep up with the competition, organizations must design and create safe environments in which business process and procedures can function. These environments must maintain confidentiality and privacy and assure the integrity of organizational data-objectives that are met through the application of the principles of risk management.

Accountability for Risk Management

- It is the responsibility of each community of interest to manage risks. Each community has a role to play :
  - *Information security* best understands the threats and attacks that introduce risk into the organization.
  - *Management and users* play a part in the early detection and response process. They also ensure sufficient resources are allocated.
  - *Information technology* must assist in building secure systems and operating them safely.
- All three communities must also :
  - Evaluate the risk controls.
  - Determine which control options are cost effective.
  - Assist in acquiring or installing needed controls.
  - Ensure that the controls remain effective.
- Further, managers of all levels are accountable on a regular schedule for ensuring the ongoing effectiveness of every control deployed.

Scanned by CamScanner

Risk Management Process

- Management reviews asset inventory.
- The threats and vulnerabilities that have been identified as dangerous to the asset inventory must be reviewed and verified as complete and current.
- The potential controls and mitigation strategies should be reviewed for completeness.
- The cost effectiveness of each control should be reviewed as well, and the decisions about deployment of controls revisited.

Components of Risk Management

The three components of risk management process are :

(1) ***Risk Identification*** : It is the process of examining and documenting the security posture of an organization's information technology and the risk it faces.

(2) ***Risk Assessment*** : It is the documentation of the results of risk identification.

(3) ***Risk-Control*** : It is the process of applying controls to reduce the risks to an organization's data and information systems.

Fig. (3) shows these components and their inter-relationship.

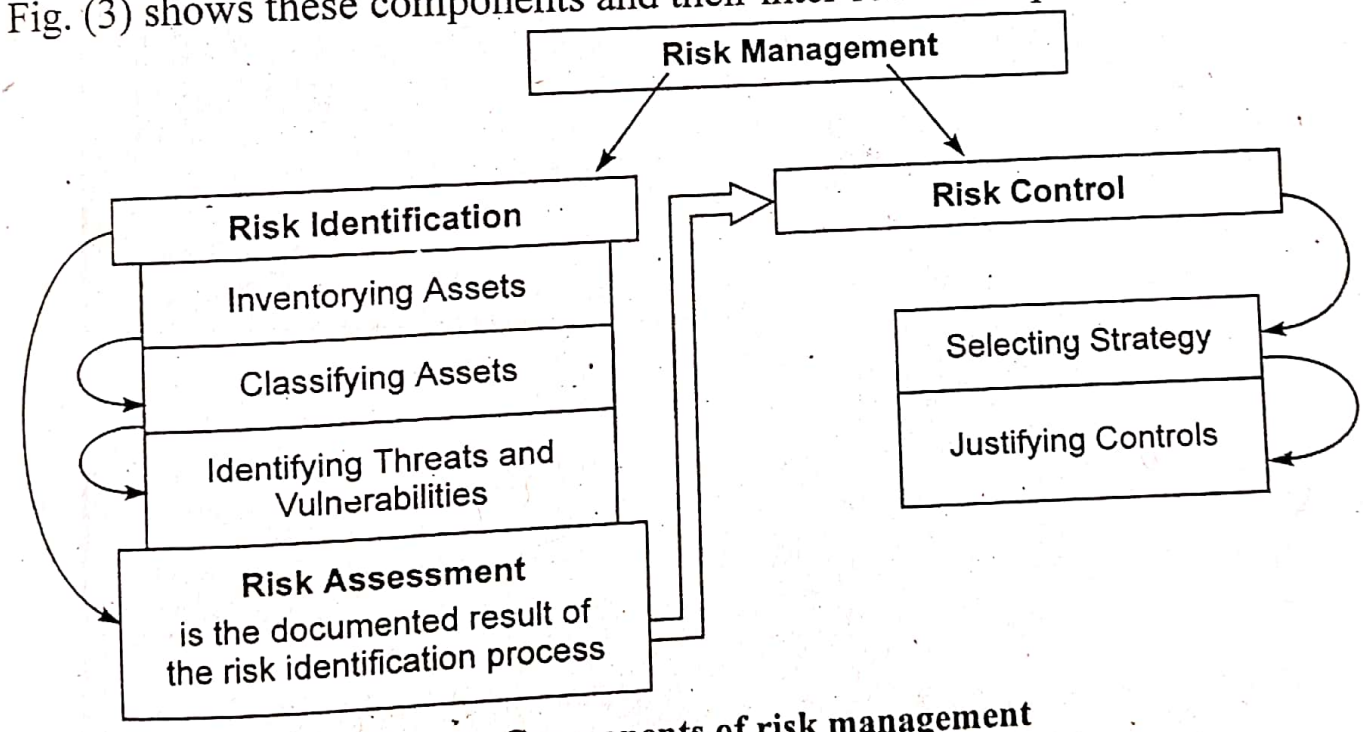

Fig. (3) Components of risk management

We now discuss these components in detail

Scanned by CamScanner