Chapter 2

Fundamentals of Information Systems Security

Objectives

- Understand Fundamentals of security
- Understand key components of IS Security
- Be able to analyze the principles of information Systems security.
- Be able to analyze the types of security controls.
- Understand what Policies, Standards and Procedures are in IS security
- Understand How to Plan , design, Implement and Administer Secured Systems

IS Security Fundamentals

- **Information Security is a Process**
  - Bruce Schneier, one of the world's most well-known experts on security, once wrote that "security is a process, not a product."
  - Indeed, with all the changing variables and players, security is a never-ending evolutionary process, wherein defenses change in response to new threats and new threats emerge with the introduction of new systems and defenses.

Key Components of Information System Security Program- 4 Components

- **Program Initiation:** This component
  - Identifies relevant stakeholders
  - determines who receives the security metrics
  - what information they require to discharge their responsibility
  - Security Requirement identification

Key Components of Information System Security Program- 4 Components

- **Developing information security metrics:** This is used to design the Security policy and the security controls.-consists of two major activities:
  - Identification and definition of the current IT security program/Policy and
  - Development and selection of specific metrics to measure the implementation, efficiency, effectiveness, and the impact of the security controls.

Key Components Cont'd...

- **Reporting information security metrics:** This component analyzes how information security metrics can be used to demonstrate "compliance with security requirements (e.g., policy and procedures),
  - Measure Compliance with the Security Program/Policy.
- **Maintaining an information security metrics program:** Once an information security metrics program is deployed, the process is not over.
  - Continuous Monitoring and Evaluation is important so that the metrics can be changed with changing security environment and defense mechanism
  - Fine tuning the Metrics

Principles of Information Security

- Information security deals with three basic issues: the confidentiality, integrity, and availability of information.
- Indeed, all the principles, standards, and mechanisms you will encounter are dedicated to these three abstract but fundamental goals of confidentiality, integrity, and availability of information and information processing resources—also referred to as the C-I-A triad or information security triad.

Principles Cont'd...

- The following are some of the major principles of Information Security
  - Principles of least privilege
  - Defense in Depth
  - Minimization
  - Compartmentalization.
  - Keep Things Simple
  - Fail Securely
  - Cost-Benefit Analysis
  - Secure the weakest link

Least Privilege

- The principle of least privilege stipulates, "Do not give any more privileges than absolutely necessary to do the required job". The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage. Examples
  - **Giving users read only access** to shared files if that's what they need, and making sure write access is disabled
  - **Not allowing help desk staff** to create or delete user accounts if all that they may have to do is to reset a password

Defense in depth

- The principle of defense in depth is about **having more than one layer or type of defense.** The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is. But two or more layers are much more difficult to breach. Defense in depth works best when you combine two or more different types of defense mechanisms—such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN.
- In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

Minimization

- The minimization principle is similar to the least privilege principle and mostly *applies to system configuration instead of the user privileges*. The minimization principle says "do not run any software, applications, or services that are not strictly required to do the entrusted job."
- To illustrate, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.

Compartmentalization

- Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment has Malfunctioned or compromised.
- Applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment.
  - From the Concept of Compartments in large Ships

Keep things simple

- Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
- The more complex a system is, the less assurance we may have that it will function as expected.
- Security doesn't work by obscurity(hiding).

Fail Securely

- Failing securely means that if a **security measure or control has failed** for whatever reason, **the system should not be rendered to an insecure state**.
- For example, when a firewall fails, it should default to a "deny all" rule, not a "permit all."
- However, fail securely does not mean "**close everything**" in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire it should default to "open doors" to help trapped in humans get out of the building.
- Main Objective is to secure even when in a failed state.

Cost-Benefit Analysis

- Although not strictly a principle, the cost-benefit analysis is a must when considering implementation of any security measure. It says that the overall benefits received from a particular security control or mechanism should clearly exceed its total costs;
- i.e The value of the Information protected should be more than the cost we incur to protect it; otherwise, implementing the security control would make no sense.
- This may sound like simple common sense, and it probably is; nevertheless, this is an important and often overlooked concern

Secure the Weakest link

- Your network may be protected by firewalls, intrusion detection and other state-of-the-art security technologies. And yet, all it takes is one person's carelessness, and suddenly it's as if you have no network security at all.
- The moral of that story is clear: No matter how secure your network may be, it's only as secure as its weakest link. And people--meaning you and your employees--are often the weakest link. It's important to note that poor security puts your business, as well as your partners, at risk. As a result, many enterprises and organizations, such as credit-card companies, now specify and require minimum levels of security you must have in order to do business with them.

Types of Information System security Controls

Types of IS security Controls

- Central to information security is the concept of controls, which may be categorized
- By their functionality in order
  - Preventive Control
  - Detective Control
  - Corrective Control
  - Deterrent Control
  - Recovery Control
  - Compensating Control
- By the Plan of application
  - Physical,
  - Administrative
  - Technical.

Preventive controls

- Preventive controls try to prevent security violations and enforce ***access control***
- Like other controls, preventive controls may be physical, administrative, or technical:
  - Doors- physical preventive control
  - security procedures- administrative preventive control
  - Authentication-Technical preventive controls

Detective Controls

- Detective controls are in place to detect security violations and alert the defenders. They come into play when preventive controls have failed or have been by-passed.
- Detective controls include cryptographic checksums, file integrity checkers, audit trails and logs, and similar mechanisms.
  - But, how do you know if you are being passively attacked? say by a spyware.

Corrective Controls

- Corrective controls try to correct the situation after a security violation has occurred. Although a violation has occurred, not all is lost, so it makes sense to try and fix the situation.
- Corrective controls vary widely, depending on the area being targeted, and they may be technical or administrative in nature.
  - What will you do if you lost a key to your Data center?

Deterrent Controls

- Deterrent controls are intended to *discourage potential attackers* and send the message that it is better not to attack, but even if you decide to attack we are able to defend ourselves.
- Examples of deterrent controls include notices of monitoring and logging as well as the visible practice of sound information security management.

Recovery Controls

- Recovery controls are somewhat like corrective controls, but they are applied in more serious situations to ***recover*** from security violations and ***restore information*** and ***information processing resources***.
- Recovery controls may include disaster recovery and business continuity mechanisms, data backup systems and, emergency key management arrangements etc.
  - Eg Cockpit Lockouts

Compensating controls

- Compensating controls are intended to be alternative arrangements for other controls
- Used when the original controls have failed or cannot be used.
- When a second set of controls address the same threats that are addressed by another set of controls, the second set of controls are compensating controls

Access Control Models

Access Control Models

- Logical access control models are the abstract foundations upon which actual access control mechanisms and systems are built. Access control is among the most important *concepts in computer security.* (as is policy to information Security).
- Access control models define how computers enforce access of subjects (such as users, other computers, applications, and so on) to objects (such as computers, files, directories, applications, servers, printers, and devices).

Types of Access Control Models

- The access control model enables you to control the ability of a process to access securable objects or to perform various system administration tasks.
- Four main access control models exist:
  - (DAC)- The discretionary access control model
  - (MAC)-The mandatory access control model
  - (RBAC)-The role-based access control model
  - (RB-RBAC)- The Rule-based Access Control Model

Discretionary Access Control (DAC)

- Discretionary Access Control (DAC)
  In DAC, the data owner determines who can access specific resources. DAC allows each user to **control access** to their own data. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions. DAC allows an individual complete control over any objects they own along with the programs associated with those objects.
- Role-Based Access Control (RBAC)
  RBAC allows access based on the job title. **RBAC** is a method of restricting network access based on the roles of individual users within an enterprise. **RBAC** lets employees have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't **pertain** to them. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.

Discretionary Access Control (DAC)

- Rule-Based Access Control (RAC)
  Rules Based Access Control, **access** is allowed or denied to resource objects **based** on a set of **rules** defined by a system administrator. For example, if someone is only allowed access to files during certain hours of the day, Rule Based Access Control would be the tool of choice.
- Mandatory Access Control (MAC)
  In MAC, users do not have much freedom to determine who has access to their files. A**ccess** to system resources is **controlled** by the operating system (under the **control** of a system administrator

Discretionary Access Control (DAC)

- The discretionary access control model is the most widely used of the three models.
- In the DAC model, the owner (creator) of information (file or directory) has the **discretion** to decide about and set access control restrictions on the object in question.
- DAC is a means of restricting **access** to objects based on the identity of subjects and/or groups to which they belong.
- In DAC, the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions

MAC- Mandatory Access Control

- Mandatory access control, as its name suggests, takes a stricter approach to access control.
- Users have little or no discretion as to what access permissions they can set on their information.
- MAC-based systems use data classification levels (such as public, confidential, secret, and top secret) and security clearance levels corresponding to data classification levels to decide what access control restrictions to enforce
- This Models works in accordance with the system wide security policy set by the system administrator.
- Data has a classification level and Users have a clearance Level.

Role-Based Access Control (RBAC)

- In the role-based access control model, rights and permissions are assigned to roles instead of individual users. **This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.**
- For example, access to marketing files may be restricted to the marketing manager role only, and users Ann, David, and Joe may be assigned the role of marketing manager. Later, when David moves from the marketing department elsewhere, it is enough to revoke his role of marketing manager; no other changes would be necessary.
- When you apply this approach to an organization **with thousands of employees and hundreds of roles,** you can see the added security and convenience of using RBAC.

Rule-Based Access Control (RB-RBAC)

- Rule Based Access Control, also with the acronym RBAC or RB-RBAC.
- Rule Based Access Control will dynamically assign roles to users based ***on criteria*** defined by the custodian or system administrator.
- For example, if s***omeone is only allowed access to files during certain hours of the day, Rule Based Access Control would be*** the tool of choice.
- The additional "rules" of Rule Based Access Control requiring implementation may need to be "programmed" into the network by the custodian or system administrator in the form of code versus "checking the box."

Centralized vs. Decentralized Access Control

- Centralized access control enables the user to access all applications, websites and other computing systems from a single profile, with the same credentials from any location.
- Decentralize access control enables users to provide different credentials (usernames and passwords) for any application or website they access

IS Security:
Policies, Standards and Procedures

IS Security: Policies, Standards and Procedures

- **Policy** is a high-level statement of enterprise beliefs, goals and the general means for their attainment
- **Standards** are mandatory requirements that support individual policies
- **Procedures** are mandatory step-by-step, detailed actions required to complete a task successfully.
- **Guidelines** are similar to standards but are not mandatory.

Policy and Procedure Cont'd...

- The objective of an information security is to protect the integrity, confidentiality and availability of the information
- An information protection program should be part of an overall asset protection program
- Information security policies, standards and procedures enable organizations to
  - Ensure that their security policies are properly addressed
  - Every employee knows what s/he needs to do to insure the information security of the company

Developing policies: A good policy should

- Be Easy to understand (By all people who will have to read the policy)
- Be Applicable (Don't copy others' policy word by word since it may not be applicable to you)
- Be Do-able (The restrictions should not stop work!)
- Be Enforceable (If it cannot be enforced, it will probably remain on paper)
- Be Phased in (Organizations need time to digest policy)
- Be Proactive (Say "what is allowed" rather than "what is not allowed")
  - Organizations think:
    - Anything that is not permitted is prohibited
  - User think:
    - Anything that is not prohibited is permitted

A Good Policy Cont'd…

- Avoid absolutism (Be diplomatic)
- Meet business objectives
  - Must balance Access and Security.
  - Should lower the security risks to a level acceptable by the organization without hampering the work of the organization to an unacceptable level

Developing policies: There are three types (Tiers) of policies

- Global policies (Tier 1)
  - Used to create the organization's overall vision and direction
  - An Enterprise information security policy (EISP)
- Topic specific policies (Tier 2)
  - Address particular subject of concern
  - the issue-specific security policy (ISSP)
    - Ex. Antivirus, E-mail
- Application-specific policies (Tier 3)
  - Decisions taken by management to control particular applications
  - System-specific security policies (SysSPs)
    - Ex. Accounting system, HR System , Supply Chain Management System… etc.

Developing standards

- Standards define what is to be accomplished in specific terms
- Every industry has standards that try to **insure some quality of product or service, or enable interoperability**
- Many industry standards have information security issues
  - Ex. Banking, Healthcare
- Some of the standards become national regulations and organizations will have to follow that
- Organizations can also develop their own standards (enterprise standards)
- Standards are easier to update than global policies
- Standards have to be reviewed regularly.

Developing standards cont'd...

- Standards must be
  - Reasonable
  - Flexible
  - Current
  - Practical
  - Applicable
  - Reviewed regularly
- Standards should enable the enterprise to fulfill its business objectives while minimizing the security risks

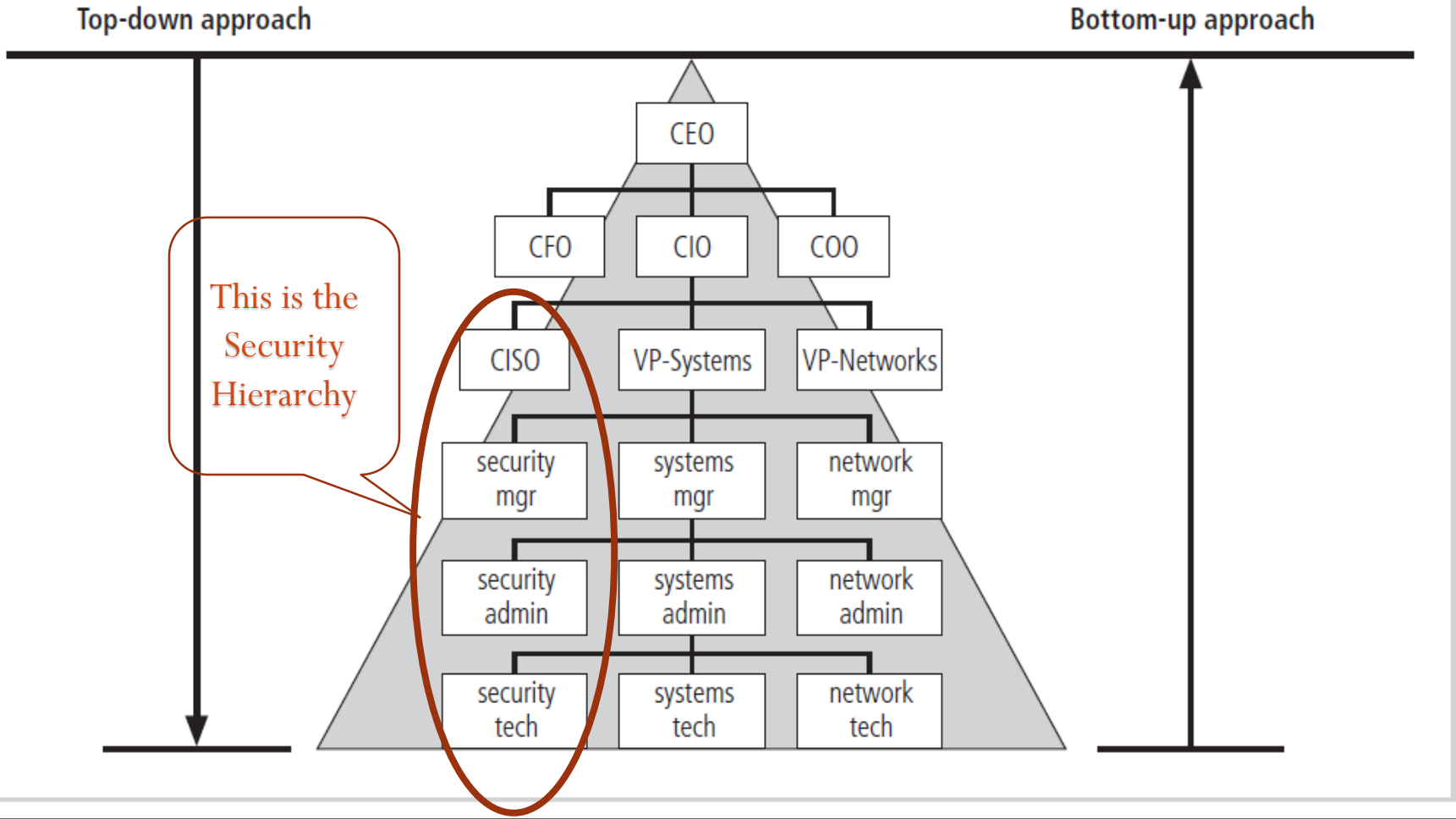
Developing Procedures

- Developing a procedure should be faster than developing a policy since it does not need to be approved by management
- The best way to write a procedure is to use a technical writer (different from the subject matter expert – SME)
- Procedure writing process (what is procedure ?)
  - Interview with the SME
  - Preparation of a draft
  - Review of the draft by the SME
  - Update of the procedures based on the comments
  - Final review by SME
  - Update of the procedures based on the comments
  - Testing of the procedures
  - Publishing of the procedures
- The procedures should also be reviewed regularly

IS Security Governance

- Governance of Information security is a part of information systems governance
- Introduces a new position under the CIO.
  - CISO- Chief Information Security Officer
    - Is the head of Information Security in an organization.
  - Security manager
  - Security Administrator
  - Security Technician

Organizational structure for security Implementation



The IS Security Governance Hierarchy

- The Chief information security officer (CISO) has primary responsibility for the assessment, management, and implementation of information security systems in the organization.
- The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two.
- However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals.

Planning, Designing and Implementing and Monitoring Secured systems

- Usually security considerations are underestimated in the Development of an Information System.
- Information Systems are developed using a standard development approach -SDLC
- The development approach doesn't include security considerations
- Recently, there have been some organizations working on an Information Security Frameworks.
- The well-known security frame work is C&A (Certification and Accreditation) process of NIST (National Institute of Standards and Technology) of USA

SecSDLC- Phases

- The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project.
- While the two processes may differ in intent and specific activities, the overall methodology is the same. At its heart, *implementing information security* involves identifying specific threats and creating specific controls to counter those threats.
- The SecSDLC unifies this *process* and makes it a coherent program rather than a series of random, seemingly unconnected actions.
- Other organizations use a *risk management approach* to implement information security systems.

C&A: Phases/Process to secured SDLC

C&A

- **Certification and Accreditation (C&A)** is a process for implementing information security.
- It is a systematic procedure for evaluating, describing, testing and authorizing systems prior to or after a system is in operation.
- The C&A process is used extensively in the U.S. Federal Government.

C&A: what are they?

- **Certification** is a comprehensive evaluation of the technical and non-technical security controls (safeguards) of an information system
- The evaluation supports the accreditation process and establishes the extent to which a particular design and implementation meets a set of specified security requirements.
- **Accreditation** is the formal declaration by a senior agency official (Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA)) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural security controls (safeguards).

The Secured Systems Development Process

- The Secured Systems Development Process has five basic phases which can be aligned to the Waterfall Model/SDLC phases
  - Initiation Phase
  - Development/Acquisition
  - Implementation/Assessment
  - Operational/Maintenance
  - Disposal

What we do at Initiation phase

- During this phase, security requirements at an enterprise level are identified.
- Key activities include:
  - Initial definition of business requirements in terms of confidentiality, integrity, and availability
  - Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information
  - Determination of any privacy requirements.

What we do at Development & Acquisition phase

- During this phase, technical and functional requirements are translated in to an actual plan for an information system.
- Key activities include:
  - Conduct the risk assessment and use the results to supplement the baseline security control
  - Analyze security requirements
  - Perform functional and security testing
  - Prepare initial documents for system certification and accreditation
  - Design security architecture.

What we do at Implementation/ Assessment phase

- During this phase, the system will be installed and evaluated in the organization's operational environment.
- Key activities include:
  - Integrate the information system into its operational environment
  - Plan and conduct system certification activities in synchronization with testing of security controls; and
  - Complete system accreditation activities

What we do at Operations/Maintenance Phase

- In this phase,
  - systems are in place and operating,
  - enhancements and/or modifications to the system are developed and tested
  - hardware and/or software is added or replaced.
  - The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated.
  - The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient- remember IS security is a process- not an Absolute Result/Product

Operations/Maintenance…

- Key activities include:
  - Configuration management and control ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.
    - What kind of testing helps to avoid vulnerabilities due to change in an IS Component?
  - Continuous monitoring—ensures that controls continue to be effective in their application through periodic testing and evaluation.

What we do at Disposal phase

- This phase is important for disposal of a system and closeout of any contracts in place.
- When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that organizational resources and assets are protected.
- Key activities include:
  - Build and Execute a Disposal/Transition Plan;
  - Archive of critical information-preservation;
  - Sanitization of media.
  - Disposal of hardware and software.

The SDLC

SDLC	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition

	- Needs Determination:
	  ▪ Perception of a Need
	  ▪ Linkage of Need to Mission and Performance Objectives
	  ▪ Assessment of Alternatives to Capital Assets
	  ▪ Preparing for investment review and budgeting
		- Functional Statement of Need
		- Market Research
		- Feasibility Study
		- Requirements Analysis
		- Alternatives Analysis
		- Cost-Benefit Analysis
		- Software Conversion Study
		- Cost Analysis
		- Risk Management[7] Plan
		- Acquisition Planning
			- Installation
			- Inspection
			- Acceptance testing
			- Initial user training
			- Documentation
				- Performance measurement
				- Contract modifications
				- Operations
				- Maintenance
					- Appropriateness of disposal
					- Exchange and sale
					- Internal organization screening
					- Transfer and donation
					- Contract closeout

7 -Risk management in this context refers to risk associated with the development and not computer security or system technical risk.

Security Consideration in SDLC- Summary

	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition
SECURITY CONSIDERATIONS	- Security Categorization - Preliminary Risk Assessment	- Risk Assessment - Security Functional Requirements Analysis - Security Assurance Requirements Analysis - Cost Considerations and Reporting - Security Planning - Security Control Development - Developmental Security Test and Evaluation - Other Planning Components	- Inspection and Acceptance - Security Control Integration - Security Certification - Security Accreditation	- Configuration Management and Control - Continuous Monitoring	- Information Preservation - Media Sanitization - Hardware and Software Disposal