Lesson Proper for Week 11

SECURING THE CONTROL AND MANAGEMENT PLANES

The ultimate objective of network security is to protect an organization's critical and sensitive data from unauthorized access and destruction while ensuring its availability and integrity. There are many options available, so organizations can choose the one that best suits their network and business requirements. One example is the Cisco Security Manager, which helps in managing the entire deployed network. However, before understanding the various other aspects of network management, it is important to know about security policies and their components.

INTRODUCTION THE SECURITY POLICY

Any organization depending on a network has a security policy in place. A security policy basically contains the following:

- The organization's objectives
- Rules and regulations for the network's users and administrators
- Requirements for the system and management that collectively ensure network security

A security policy also lays down the guidelines, standards, and procedures for the functioning of a network. The main components of a security policy are the governing policy, the end-user policy, and the technical policy:

- **Governing policy:** This policy contains the answers to the ""what needs a security policy"" question. It contains high-level categorization of the security elements that are important for the organization. People at managerial or technical level are responsible for this policy.

· **End-user policy:** This policy contains the security requirements for the end users and also details the security policy questions of what elements need security, when it is required, and where it is required.

· **Technical policy:** These policies are more detailed compared to the governing policy ,and address only a specific issue, such as access control or physical security. This policy is used by members of the security staff.

IT governance, risk management, and compliance, referred to as IT GRC, are also significant components of a security policy. In organizations, the efforts in terms of IT governance, risk management, and compliance are often separated either by department or the type of regulation. This segregation—in order to achieve a secure IT environment that adheres to the regulatory compliance requirements—can create certain problems, such as incurring higher costs, the utilization of too many resources, and increased time and effort.

However, nowadays, organizations are working towards simplifying the process by converging the three components. This figure illustrates the convergence of the three components in an organization:

The result of this convergence, as illustrated, is an effective process to define risk based on an organization's rules and business objectives, and that comes within the framework of compliance regulations. While risk management identifies potential risks, how they occur, and determines their impact, IT governance, in addition to alleviating risks, creates rigorous prerequisites for the framework of information security.

The compliance component determines the levels of compliance and the impacts of non-compliance to the security policy. Apart from the security policy, secure network management depends on a structured approach, which is the life cycle approach. The convergence of the three components results in an ideal framework and context to create a life cycle approach to information security. It also results in reducing expenses and increasing effectiveness.

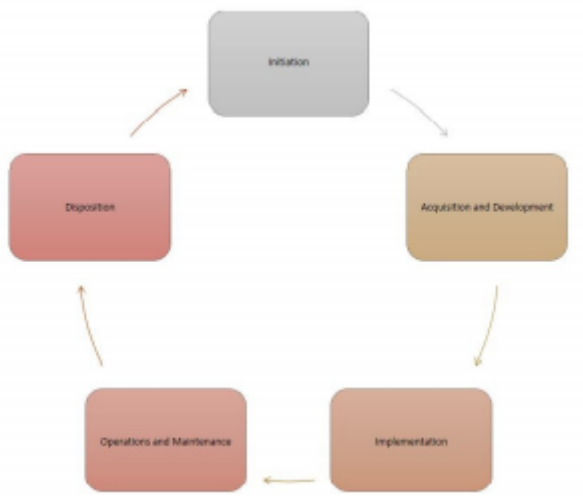
Phases of secure network life cycle

The life cycle approach to security management focuses on various elements of security, such as the assessment, testing, implementation, and monitoring phases of security. In an effort to provide a structured methodology for network security, it emphasizes and describes the roles of regulatory compliance, risks, and security policies in designing effective network frameworks.

As discussed, the components of IT governance, risk management, and compliance, forming the core of the security framework, ensure an economical and efficient process. Including the security component while in the **system development life cycle (SDLC)** helps with less expensive and less effective security. The SDLC contains five ph

They are as follows:

- **Initiation**
- **Acquisition and Development**
- **Implementation**
- **Operations and Maintenance**
- **Disposition**



1. Initiation Phase

During this phase, an organization states the need for systems and plans the systems' security by identifying the key security roles. Apart from evaluating the information that need to be stored, transmitted, or processed, the confidentiality, integrity, and availability of information should also be assessed. The initiation phase includes the two components.

2. Acquisition and Development Phase

In this phase, the system is designed, programmed, and developed. It has five key components.

3. Implementation Phase

In this phase, the security features are configured, their functionality tested, and they are installed. Finally, a formal certification or authorization is obtained to operate the system. The authorization ensures that the system is functioning as per the established techniques and procedures. It is also seen as an assurance that the required safety measures are in place to protect the organization's information.

4. Operation and Maintenance Phase

In this phase, the security features are configured, their functionality tested, and they are installed. Finally, a formal certification or authorization is obtained to operate the system. The authorization ensures that the system is functioning as per the established techniques and procedures. It is also seen as an assurance that the required safety measures are in place to protect the organization's information.

5. Disposal Phase

In this phase, the security features are configured, their functionality tested, and they are installed. Finally, a formal certification or authorization is obtained to operate the system. The authorization ensures that the system is functioning as per the established techniques and procedures. It is also seen as an assurance that the required safety measures are in place to protect the organization's information.

However, the utmost care is required when choosing the disposal method, to avoid the unauthorized disclosure of sensitive data.

◀ Preliminary Activity for Week 11 Jump to... Analysis, Application, and Exploration for Week 11 ▶

Navigation

Home
Dashboard
Site pages
My courses
121 - CC106
121 - BPM101 / DM103
121 - OAELEC2
121 - ITE3
121 - MUL101
121 - ITSP2B
Participants
Grades
General
01 Exploring Security Threats
02 Delving into Security Toolkits
03 Intrusion Prevention System
04 Understanding Security Policies I
05 Understanding Security Policies II
06 - Preliminary Examination
07 Deep Diving into Cryptography
08 Deep Diving into Cryptography: Types of Cipher
09 Implementing the AAA Framework
10 Implementing the AAA Framework: Implementing A...
11 Securing the Control and Management Planes
Preliminary Activity for Week 11
Lesson Proper for Week 11
Analysis, Application, and Exploration for Week 11

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

Activities

- Assignments
- Forums
- Quizzes
- Resources