Nama : Yulia Oktaviani

NIM : F1E115015

UJIAN TENGAH SEMESTER (UTS)
MANAJEMEN RESIKO KEAMANAN INFORMASI

1. Review Question hal 31-32, pilih 4 dari 20 soal untuk kalian kerjakan

✓ What is information security ? What essential protections must be in place to protect information system from danger ?

Answer : Information security can define as the protection of information and its critical characteristics such as confidentiality, integrity and availability that include the systems and hardware that use store and transmit that information, throught the application of policy, training and awareness programs, and technology. InfoSec includes the broad areas is computer, data and network security.

Specialized area of security include :

a. Physical security (protecting people, assers and workplace from various threats, including fire and natural disaster

b. Operation security (protecting the organization’s communication’s ability to carry out its operational activitiew without interruption or compromise)

c. Communications security (protecting the organization communications media, technology and content and its ability to use these tools to achieve the organization’s objective)

d. Network security (protecting the organization’s data networking device, connection and contents)

✓ Define the InfoSec processes of identification, authentication, authorization, and accountability?

Answer :

a. Identification an information system possess characteristic of can identification when it is able to recognize individual users. Identification is the first step in gaining access to secured material and it serves as the foundation for subsequent authentication and authorization. Identification is typically performed by means of a username or other ID

b. Authentication means as process by which a control establishes whether a user of system has the identity it claims to have. Examples include the use of cryotographic certificates to establish Secure Sockets Layer (SSL) connections as well as the use of cryptographic hardware device for example, hardware tokens such as RSA’s SecurID.

c. Authorization is the second process after the user is authenticated, a process called authorization defines what the user (whether a person or a computer) hass been specifically and explicitly authorized by the proper authority to do, such as access, modify, or delete the content of an information asset.

d. Accountability of information occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.

✓ What are the three types of general planning? Define each

Answer :

a. Stratgeic planning (This occurs at the highest levels of the organization and for a long period of the time, usually five or more years.

b. Tactical planning (This focuses on production planning and integrates organizational resource at a level below the entire entreprise and for an intermediate duration (such as one to five years)

c. Operational planning (This focuses on day-to-day operations of local resources and occurs in the present or the short term.

✓ List and describe the five steps of general proble solving process?

Answer :

1. Recognize and define the problem, first step to solving problem is recognize and define the problem, the most frequent flaw in problem solving is failing to define the problem completely. Begin by clearly identifying exactly which problem needs to be solved.
2. Gather Facts and make assumption, the next step is understand the background and events that’s shape the problem, a manager can gather facets about the organizational,

cultural, technological, and behavioral factors that are at the root of the issue. The manager can make assumption about the methods that are availbale to solve the problem.

3. Develop possible solutions, after make assumption the next step is to begin formulating possible solutions. Managers can use several method to generate ideas. On of these is brainstorming, a process in wiich a group of indivials air as many ideas as possible in short time, without regard for their practicality.
4. Analyze and Compare Possible Solutions, Each proposed solution must be examined and ranked as to its likely success in solving the problem.
5. Select, Implement and Evaluate, Once a solution is chosen and implemented, you must evaluate it to determine its effectiveness in solving the problem

2. Review Question hal 68-69, pilih 3 dari 20 soal untuk kalian kerjakan

- ✓ What is planning ? How does an organization determine if planning is necessary?

  Answer : Planning define as central to the management of any organization and based on the preparation, application, control of sequence of action steps to achieve specific goals. Planning provides direction for the organization’s future. Without specific and detailed planning, organizational units would attempt to meet objectives independently, with each unit being guided by its own initiatives and ideas. Organizational planning should make use of a top-down process in which the organization’s leadership chooses the direction and initiatives that the entire organization should pursue. Initially, the organizational plan contains few specific detailed objectives; instead, it outlines general objectives.

- ✓ What are the five basic outcomes that should be achieved through InfoSec governance?

  Answer :

  a) Strategic alignment of InfoSec with business strategy to support organizational objectives
  b) Risk management by executing appropriate measures to manage and mitigate threats to information resources
  c) Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively

d) Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure that organizational objectives are achieved

e) Value delivery by optimizing InfoSec investments in support of organizational objectives

- ✓ Who are stakeholder? Why is it important to consider their views when planning ?

  Answer : Stakeholder is used to describe those entities, whether people or organizations, that have a stake or vested interst in a particular aspect of the planning or operation of the organizations. Stakeholders are typically asked for input whenever strategic decisions affecting their "stake" are planned. When planning, members of the InfoSec community of interest use the same processes and methodologies that the general management and IT management communities of interest use. Because the InfoSec community of interest seeks to influence the entire organization, an effective InfoSec planner should know how the organizational planning process works so that participation in this process can yield measurable results.

3. Review Question hal 118-119, pilih 2 dari 20 soal untuk kalian kerjakan

- ✓ What is alert roster? What is an alert message? Describe the two ways they can be used.

  Answer : An alert roster is a document containing contact information on the individuals to be notified in the event of an actual incident. The alert message is a scripted description of the incident and consists of just enough information so that each responder, CSIRT or otherwise, knows what portion of the IR plan to implement without impeding the notification process. There are two ways to activate an alert roster: sequentially and hierarchically. A sequential roster requires that a contact person call each and every person on the roster. A hierarchical roster requires that the first person call designated people on the roster, who in turn call designated other people, and so on.

- ✓ What is incident damage assessment? What is it used for?

  Answer : Incident demage assessment is The immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets. The damage can range from minor (a curious hacker snooping around) to severe (hundreds of computer systems infected by malware). System logs, intrusion detection logs, configuration logs, and other documents, as well as the documentation from the incident response, provide information on the type, scope, and extent of damage.

4. Exercise hal 157-158, pilih 1 dari 5 soal untuk kalian kerjakan

- ✓ Search for sample security policies on the Web. Identify five EISP and five ISSP sample policies and bring them to class. Compare these with the framework presented in this chapter and comment on the policies' comprehensiveness.

  Answer :

  1. EISP Policy
     a. Information Technology is a means of computers used, telecommunications and other means of electronics processing of financial data and or banking services.
     b. Banking Services Through Electronic Media or hereinafter referred to Electronic Banking is a service that allows banks to gather information, communicate, and perform banking transactions through electronic media such as ATMs, telephones banking, electronic funds transfers, internet banking, mobile phones.
     c. Strategic Plan of Information Technology (Information Technology Strategy) Plan is a document that reflects the vision and mission of Technology Information Bank, a strategy that supports that vision and mission and the main principles that become the reference in the use of Technology
     d. Data Center (Data Center) is the main facility of data processing Bank which consists of hardware and software to support activities Bank operations continuously.
     e. Disaster Recovery Center (DRC) is a replacement facility at the time of the Center Data (Data Center) is interrupted or can not work between others due to the absence of electricity to the computer room, fire, explosion or damage to the computer, which is used temporarily during the recovery of the Bank Data Center to maintain business continuity.

  2. ISSP Policy

a. Banks are required to apply risk management effectively in the use of Information Technology.

b. Application of risk management as referred to in paragraph (1) at most less include:

    1. active supervision of the Board of Commissioners and the Board of Directors;
    2. adequacy of policies and procedures for the use of Information Technology;
    3. the adequacy of the process of identification, measurement, monitoring and
    4. risk control of the use of Information Technology; and
    5. internal control system for the use of Information Technology.

c. Application of risk management as referred to in paragraph (1) at most less include:

    1. active supervision of the Board of Commissioners and the Board of Directors;
    2. adequacy of policies and procedures for the use of Information Technology;
    3. the adequacy of the process of identification, measurement, monitoring and
    4. risk control of the use of Information Technology; and
    5. internal control system for the use of Information Technology.

d. Implementation of risk management must be done in an integrated manner each stage of the use of Information Technology since the planning process, procurement, development, operation, maintenance until termination and the elimination of Information Technology resources.

e. Application of risk management in the use of Information Technology by the Bank as referred to in Article 2 shall be adapted to the objectives, business policies, size and complexity of the Bank's business.

Between the policies of the companies that have been discussed with the framework is almost same. There is no difference, it is only adjusted to the needs of the company itself.