# CNSS Security Model

Each cell represents an area of intersection among three dimensions that must be addressed to secure information systems

When using this model to design or review any information security program, you must make sure that each of the 27 cells is properly addressed by each of three communities of interest.

# What is security?

Security is defined as “the quality or state of being secure—to be free from danger”

# What is information security?

The protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information.

# Key concepts explained.

**C.I.A:**

**a) Confidentiality**: The characteristic of information whereby only those with sufficient privileges may access certain information

**b) Integrity**: Integrity ensures that data cannot be modified without being detected.

**c) Availability:** The characteristic of information that enables user access to information in a required format, without interference or obstruction

**Privacy**: Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected

**Identification**: An information system possesses the characteristic of identification when it can recognize individual users

**Authentication**: Occurs when a control proves that a user possesses the identity that he or she claims

**Authorization**: Authorization occurs after the identity of a user is authenticated

**Accountability**: Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process

**Policy**: The set of organizational guidelines that dictates certain behavior within the organization

# Program Evaluation and Review Technique (PERT)

Most popular technique

Originally developed in the late 1950’s for government-driven engineering projects

# Project Management (cont’d.)

# What is management?

The **process** of achieving objectives using a given set of resources.

(1) Identifying and controlling the resources applied to the project

(2) Measuring progress

(3) Adjusting the process as progress is made

**Managerial roles**

* + Informational role
  + Collecting, processing, and using information that can affect the completion of the objective.
  + Interpersonal role
  + Interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task.
  + Decisional role
  + Selecting from among alternative approaches, and resolving conflicts, dilemmas, or challenges.

This distinction between a leader and a manager is important because leaders do not always perform a managerial function, whereas nonmanagers are often assigned leadership roles. However, effective managers are also effective leaders.

# 88849_01_F03.jpgWhat is POLC and how does it work?

**Planning** process begins with the creation of strategic plans for the entire organization, then divided up into planning elements

**Organizing** dedicated to the structuring of resources to support the accomplishment of objectives

**Leadership** encourages the implementation of the planning and organizing functions

**Control** function serves to assure the organization of the validity of the plan

**Three levels of planning**

* + Strategic: long period of time, five or more years
  + Tactical: intermediate duration, one to five years
  + Operational: day-to-day operations

**Goals and objectives**

* + Goals are the end results
  + Objectives are intermediate points that allow you to measure progress toward the goal

**Solving Problems**

* Step 1: Recognize and define the problem
* Step 2: Gather facts and make assumptions
* Step 3: Develop possible solutions
* Step 4: Analyze and compare possible solutions
* Step 5: Select, implement, and evaluate a solution

# Principles of Information Security Management

The extended characteristics of information security are known as the six P’s.

What are the unique functions of InfoSec management known as “the six Ps”?

**Planning**

* Core components of project plan
  + Work time, resources, and project deliverables
* Types of InfoSec plans
  + Incident response planning
  + Business continuity planning
  + Disaster recovery planning
  + Policy planning
  + Personnel planning
  + Technology rollout planning
  + Risk management planning
  + Security program planning

**Policy**

Enterprise information security policy (EISP)

Sets the tone for the InfoSec department across the organization.

EISP is used to determine the scope, tone and strategic direction for a company and all the security-oriented topics within. This policy should directly reflect the goals and mission of the company.

Issue-specific security policy (ISSP)

Sets of rules of acceptable behavior within a specific technology

guide employees on the use of specific types of technology

System-specific policies (SysSPs)

Technical in nature and control the equipment or technology.

The SysSP should be designed and created focus on a specific type of system

**Programs**

InfoSec operations that are specifically managed as separate entities

**Protection**

Executed through risk management activities

**People**

The most critical link in the information security program

Managers must recognize the crucial role that people play in the information security program

**PM**

Identifying and controlling the resources applied to the project

Measuring progress

Adjusting the process as progress is made

# Why and how the project management is applied to security?

**WHY?**

* Information security is a process, not a project
  + Each element of an information security program must be managed as a project
  + A continuous series, or chain, of projects
* Some aspects of information security are not project based
  + They are managed processes (operations)
  + Monitoring internal/external environments, ongoing risk assessments, continuous vulnerability assessment.
  + Involves the temporary assemblage resources to complete a project
  + Some projects are iterative, occurring regularly (e.g., budgets)

InfoSec work often involves collaboration across departments and PM offers a way to effectively organize and guide these resources.

**HOW?**

* First identify an established project management methodology
* PMBoK (Project Management Body of Knowledge) offers a structured, standardized approach to InfoSec management.

By implementing PM, InfoSec benefits from an organized approach, ensuring security measures are effectively executed, risks are appropriately managed, and resources are efficiently use.

Although InfoSec is a process, not a project, each element of an InfoSec program must be managed as a project.

# Fundamentals of Contingency Planning

Incident response planning (IRP)

Focuses on immediate response

Disaster recovery planning (DRP)

Focuses on restoring operations at the primary site after disasters occur

Business continuity planning (BCP)

Facilitates establishment of operations at an alternate site

# What is contingency planning and why is it important?

**Contingency planning:** The overall planning for unexpected events.

Involves preparing for, detecting, reacting to, and recovering from events that threaten the security of information resources and assets.

**Main goal:** The restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event.

# What are the three types of contingency plan and what are their respective usage context?

**Incident response planning (IRP):** Focuses on immediate response

**Disaster recovery planning (DRP):** Focuses on restoring operations at the primary site after disasters occur

**Business continuity planning (BCP):** Facilitates establishment of operations at an alternate site, until the organization can resume operations at its primary site or select a new primary location

**Why DR important:**

The disaster recovery plan is critical to the organization because it allows incidents identified by the incident response team to be escalated to the level of disaster.

**Why BC important:**

A business continuity plan ensures that critical business functions can continue if disaster occurs, and thus is essential to the survival of the organization in the event of a disaster

# How to make policies effective? (develop, distribute, review, understand, agree, enforce)

Developed using industry-accepted practices

Distributed or disseminated using all appropriate methods

Reviewed or read by all employees

Understood by all employees

Formally agreed to by act or assertion

Uniformly applied and enforced

# What roles do policies play in Infosec management?

Policy is the essential foundation of an effective information security program.

To address threats and implement strategies to mitigate IT security vulnerabilities,

To defining how to recover from a system compromise or when a network intrusion occurs.

To provide guidelines to employees on what to do and what not to do.

To define who gets access to what assets and resources, and what the consequences are for not following the rules.

# Organizing for Security:

**Variables involved in structuring an information security program**

Organizational culture

Size

Security personnel budget

Security capital budget

**As organizations increase in size:**

Their security departments are not keeping up with increasingly complex organizational infrastructures

# Implementing Security Education, Training, and Awareness Programs

**SETA program**

Designed to reduce accidental security breaches

Consists of three elements: security education, security training, and security awareness

**Awareness, training, and education programs offer two major benefits:**

Improving employee behavior

Enabling the organization to hold employees accountable for their actions

# What are the typical reporting structures in organizations of various sizes (very large, large, medium, small) and their advantages and limitations?

**Small organizations**

Commonly outsource their Web presence or electronic commerce operations

Security training and awareness is commonly conducted on a 1-on-1 basis

Policies (when they exist) are often issue-specific

**Medium-sized organizations**

Have a smaller total budget

Have same sized security staff as the small organization, but a larger need

Must rely on help from IT staff for plans and practices

Ability to set policy, handle incidents, and effectively allocate resources is worse than any other size

**Large organizations**

Security approach has often matured, integrating planning and policy into the organization’s culture

Do not always put large amounts of resources into security

They tend to spend proportionally less on security

**Very large organizations**

Security budgets often grow faster than IT budgets

Even with a large budget, the average amount spent on security per user is still smaller than any other type of organization

Does a better job in the policy and resource management areas

Only 1/3 of organizations handled incidents according to an IR plan

# What are the purposes of security education, training, and awareness programs?

Improving employee behavior

Informing about where to report policy violations

Enabling the organization to hold employees accountable for their actions

# How to make a SETA program effective?

The willingness of subordinates to participate in the training

Currency of the training to make sure they have the skill and knowledge needed to make the security program function to its optimum

The amount of funds available for the program

Management’s enthusiasm about the security program (i.e. updating when needed, etc.).

Upper management’s willingness to support the chosen security program and making sure that it is correctly implemented

# What is access control?

Regulate the admission of users into trusted areas of the organization.

# What are the key principles of access control?

**Least privilege**

The principle by which members of the organization can access the minimum amount of information for the minimum amount of time necessary to perform their required duties

**Need to Know**

Limits a user’s access to the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function

**Separation of Duties**

A control requiring that significant tasks be split up in such a way that more than one individual is responsible for their completion

# What are the categories of access control?

**First method depicts controls by their inherent characteristics**

* Preventative: helps an organization avoid an incident
* Deterrent: discourages or deters an incipient incident
* Detective: detects or identifies an incident or threat when it occurs
* Corrective: remedies a circumstance or mitigates damage done during an incident
* Recovery: restores operating conditions back to normal
* Compensating: resolves shortcomings

**NIST access control categories are based on operational impact to the organization**

* Management: Controls that cover security processes that are designed by strategic planners and routinely used to design, implement, and monitor other control systems
* Operational (or administrative): Controls that deal with the operational functions of security that have been integrated into the repeatable processes of the organization
* Technical: Controls that support the tactical portion of a security program and deal with the immediate needs of the organisation.

**The third approach describes the degree of authority under which the controls are applied:**

* Mandatory Access Controls (MACs)
* Nondiscretionary Controls
* Discretionary Access Controls (DACs)

**Mandatory Access Controls (MACs)**

* Structured and coordinated within a data classification scheme that rates each collection of information as well as each user
* These ratings are often referred to as sensitivity levels
* When MACs are implemented, users and data owners have limited control over access to information resources

**Data classification model**

The U.S. military classification scheme relies on a more complex five-level classification scheme as defined in Executive Order 12958:

Unclassified data - Generally free for distribution to the public

Sensitive but unclassified (SBU) data - For Official Use Only

Confidential data - cause damage to the national security

Secret data - cause serious damage to the national security

Top secret data - cause exceptionally grave damage to the national security

Data owners must classify the information assets for which they are responsible and review the classifications periodically

Example of classification types:

* Public—For general public dissemination,
* For official use only—Not for public release but not particularly sensitive
* Sensitive—Important information
* Classified—Essential and confidential information

**Nondiscretionary controls**

Determined by a central authority in the organization

Can be role-based or task-based

Role-based controls (RBAC) are tied to a particular user’s role in an organization

Task-based controls are tied to a particular assignment or responsibility

**Discretionary Access Controls (DACs)**

Implemented at the option of the data user

Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access the resources

Most personal computer operating systems are designed based on the DAC model

One discretionary model is rule-based access controls where access is granted based on a set of rules specified by the central authority

# What are the available access control techniques?

Something you know

Something you have

Something you are

Something you produce

# Benchmarking

Following the existing practices of a similar organization, or industry-developed standards

Can help to determine which controls should be considered

Cannot determine how those controls should be implemented in your organization

# What is benchmarking and why do organizations do benchmarking?

Benchmarking is a systematic process of comparing an organization's practices, processes, products, services, or performance metrics against those of industry peers, competitors, or best-in-class organizations.

**WHY:** To generate a security blueprint

(1) Following the existing practices of a similar organization, or industry-developed standards

(2) Can help to determine which controls should be considered

(3) Cannot determine how those controls should be implemented in your organization

# What are the categories of benchmarking? (due care/due diligence, recommended practices)

(1)    Standards of due care/due diligence

(2)    Best practices

* Standard of due care
  + When organizations adopt minimum levels of security for legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances
* Due diligence
  + Implementing controls at this minimum standard
  + Requires that an organization ensure that the implemented standards continue to provide the required level of protection
  + Failure to demonstrate due care or due diligence can expose an organization to legal liability
    - If it can be shown that the organization was negligent in its information protection methods

Best Practices, include a sub-category of practices, called the gold standard, that are generally regarded as “the best of the best”

* + Security efforts that seek to provide a superior level of performance in the protection of information
  + Considered among the best in the industry
  + Balance the need for information access with the need for adequate protection
  + Demonstrate fiscal responsibility
  + Companies with best practices may not be the best in every area

# What are the benefits and limitations of benchmarking?

Benefits： Performance Improvement, Competitive Advantage, Learning and Innovation, Enhanced Decision Making

Limitations: Organizations don’t talk to each other

# What is baselining and why do organizations do baseline?

A value or profile of a performance metric against which changes in the performance metric can be usefully compared

Baseline measurements of security activities and events are used to evaluate the organization’s future security performance

# What is performance measurement and why do organizations do performance measurement?

Performance measurement refers to the process of assessing and quantifying the costs, benefits and performance of InfoSec.

Performance measurement helps organizations evaluate, monitor, and improve performance, make informed decisions, foster accountability and transparency, motivate employees, and identify areas for benchmarking and improvement.

# Risk management

Information security departments are created primarily to manage IT risk

Managing risk is one of the key responsibilities of every manager within the organization

In any well-developed risk management program, two formal processes are at work

Risk identification and assessment

Risk control

# What is risk management?

The process of assessing the risks to an organization’s information and determining how those risks can be controlled or mitigated

# How do organisations identify and assess risks?

Plan and Organize Process

Create System Component Categories

Develop Inventory of Assets

identify Threats

Specify Vulnerable Assets

Assign Value or impact Rating to Assets

Assess Likelihood for Vulnerabilities

Calculate Relative Risk Factor for Assets

Preliminary Review of Possible Controls

Document Findings

# Terms explained(information assets, threats, vulnerabilities, etc.)

Information Assets: Information assets refer to the valuable and sensitive data, information, or resources within an organization that need to be protected.

Threats: Threats, in the context of cybersecurity, are potential dangers or risks that can exploit vulnerabilities in an organization's information assets.

Vulnerabilities: Vulnerabilities are weaknesses or flaws in an organization's systems, processes, or controls that could be exploited by threats.

# What are the results of risk assessment?

Identification of Assets

Assessment of Threats

Evaluation of Vulnerabilities

Risk Likelihood

Risk Impact

Risk Rating

Recommended Controls and Mitigation Strategies

Risk Treatment Plan

# What are the risk control strategies?

Avoidance

Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability

Transference

Shifting the risk to other areas or to outside entities

Mitigation

Reducing the impact if the vulnerability is exploited

Acceptance

Understanding the consequences and accepting the risk without control or mitigation

# Why do organisations do feasibility studies and what feasibility studies do they do?

Organizations conduct feasibility studies to assess the viability and potential success of a proposed project, initiative, or business venture. Feasibility studies are conducted to gather and analyze relevant information, evaluate different options, and make informed decisions about the feasibility, profitability, and sustainability of a particular endeavor.

Economic feasibility

Organizational feasibility

Operational feasibility

Technical feasibility

Political feasibility

# Protection Mechanism----Typical protection mechanisms explained

Access control

Firewall

IDPS

Cryptography

图示

描述已自动生成

Management should integrate solid information security concepts

* Across all of the organization’s employment policies and practices
* Including information security responsibilities into every employee’s job description and subsequent performance reviews
  + Can make an entire organization take information security more seriously

# Describe the security considerations in the process of employment.

**Hiring**

**Firing**