

Framework Control

- Framework
- Controls
- Design Principle
- Security audit

Framework

Security Framework : Guidelines used for building plans to help mitigate risk and threat to data and privacy

Controls :

Safeguards designed to reduce specific security risks

① Encryption : The process of converting data from a readable format to an encoded format

② Authentication : The process of verifying who someone or something is

Biometrics : Unique physical characteristic that can be used to verify a person's identity

Vishing : The exploitation to electronic voice communication to obtain sensitive information or to impersonate a known source

③ Authorization : The concept of granting access to specific resource within system

CIA Triad (Confidentiality Integrity Availability)

Confidentiality : Only authorized user can access specific assets or data

Integrity : The data is correct, authentic and reliable

Availability : Data is accessible to those who are authorized to access it

CIA Triad is a model that help inform how ~~authorization~~ organization consider risk when setting up system and security policies

NIST Framework

Intro : NIST Cybersecurity Framework (CSF)

A voluntary framework that consist of standard, guideline and best practices to manage cybersecurity risk.

Core function

- Identify
- Protect
- Detect
- Respond
- Recover

DATE / /
PAGE

REST S.P. 800-53.

A unified framework for protecting the security of info system within the federal govt.

5 core function

Identify : Management of cyber security risk and its effect on an organization people and assets

Protect : The strategy used to protect an organization through the implementation policies procedures training and tools that help mitigate cyber security threats

Detect : Identifying potential security incident and improving capabilities to increase the speed and efficiency of detection

Respond : Making sure that the proper procedure are used to contain neutralize and analyze security incident and implement improvement the security process.

Recover : The process of returning affected system back to normal operation

Open Web Application Security project (OWASP)

Security principle

- Minimize attack surface area
- Principle of least privilege
- Defence in depth
- Separation of duties
- Keep security simple
- Fix security issue correctly

Plan a Security audit

Security audit: A review of an organization security controls policies and procedures against a set of expectations

Purpose:

- identify org. risk
- Assess control
- Correct compliance issue

Common element of internal audit:

- establish the scope and goal
- completing an ~~so risk~~ control assessment
- conducting risk assessment
- Assessing compliance
- Communicating results

• Scope refers to the specific criteria of an internal security audit

• Goals are an outline of the organization security objectives

DATE / /
PAGE

Scope : assess user permission

- identify existing control, policies and procedure
- Account for technology current in use

Goals : Adhere to the NIST CSF

- Establish policies and procedure to ensure compliance with regulation
- Fortify system control.

Risk description :

There is a lack of proper management of physical and digital assets: equipment used to store data is not properly secured and access to private info. in the org. internal network needs more robust control in place

Audit Question

- What is the audit meant to achieve
- Which assets are more at risk
- Are current control sufficient to protect these assets
- What control and compliance regulation need to be implemented

Control Categories :

- Administrative
- Technical
- Physical

Stakeholder communication : Summarize scope and goal

- List existing risks
- Provide recommendation
- Notes How quickly those risks need to be addressed
- Identifies compliance regulation