### Transwork Control

Framework
Control
Design Crinciple
Security audit

Transwork

Security Framework: Swidelines used for brilding plans to help miligate risk and brivacy

#### Controls:

Safeguards designed to reduce specific security risks

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

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

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

schooling identity

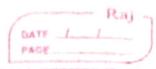
Vishing The exploitation to electronic voice

communication to obtain sensitive

information on to impersonate

a known source

(3) Authorization: The concept of granling access
to specific resource within
system:



CIA Trial (Confidentially Integrity Meridablity)

Confedentiality: Only authorized over can access specific assets or data

Islegately: The data is correct, authentic

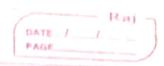
Availablely: Data is accesseble to those who are authorized to access it

CIA bried is a model that help inform how authorization organization consider susk when setting up system and security

NIST Framework

: NIST CyberSecurity Francuork (CSF) A volontary francework that consist of standard, gerdeline and best practices to manage ybersecorily risk. Core function

- · Ideality
- Protect Deled
- ·Respond
- · Recover



#### NIST S.P. 800-53.

the security of impo system within the federal good.

## 5 core function

Adenlify: Management of cylor security risk and its effect on an organization people and assets

Perotect: The strategy used to perotect an organization the implementation policies procedures training and took that help ineligate cyber security throats

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

Respond: Making swee that the peroper procedure are used to contain neutralize and analyze security incident and implement imperovement the security process.

Recover. The percess of returning affected system



# Open Web Application Security project (OWASP) · Minimize attack surface area · Perenciple of least privelage · Pefence in depth · Separation of duties · Keep Security simple · Tisc security issue correctly Plana Security audit Security audit A review of an organization security contro Purpose: identify org. risk Assess control · Correct compliance issue Common element of internal audit: establish the scope and good - completing as so rusk control assessment · conducting risk assessment · Arsessing compilance - Communicating results Scope refers to the specific criteria of an internal youls are an orlline of the gorganization security objective



Scope : assess ever permission · identify existing control, policies and procedure. Account for technology current in un Isoals: Adhere to the NIST (ST · Establish policies and procedure to ensure compliance with regulation.
· Tortify system control. Risk description:

There is a lack of proper management of physical and digeld assets: equipment used to slove data is not properly secured and access retwork needs more explorest control in place Audit auestion what is the audit meant to achieve · Which assets are more at risk · Dere current control sufficient to perolect these assets · What control and competance negotation need to be implied Control Categories: · Administrative · Ekhnica · Physical Stakeholder communication: Summarize scope and goal.

List existing risks · Perovide recommendation

Notes How girchly those risks need to be addressed. Identifies compilance regulation