Domain (1) Security & Risk management

Security

Security posture)
an organization's ability to manage it's defense of critical assets & data & react Change

(PII) → personally identifiable info

Risk mitigation :- the process of having the right procedures and rules in place to quickly reduce the impact of risk like a breach

Compliance :- primary method used to develop an organization's internal security policies & regulatory requirements & independent standards

Business continuity :-

→ Organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Sr. No.

Date :

Domain (2)

Asset security :-

focused on securing digital & physical assets

→ it also related to storage & maintenance, retention & destruction of data

It means (PII) & (SPII) should be protected and maintained

security

(PII) → personal identifiable info

(SPII) → sensitive personally identifiable info

so organization should have policies & procedures that ensure data is properly stored, maintained, retained and destroyed.

Domain (3)

security architecture & engineering :-

focused on optimizing data & security by ensuring effective tools, system, & processes are in place to protect an organization's assets and data

Share responsibity :-

all individuals with a organization take active roles in lowering risk & maintaining both physical & virtual

Date:

Sr. No.

Security

by having policies the encourage user to recognize and report securit concerns many issues.
so many issues can handle quickly & effectively

Domain 4

Communication & Network Security

→ focused on Managing and securing physical networks and wireless network communications

site or Cloud
↓
pubic wifi → Securing it
↓
networks

Domain 5 identity & access Management

→ focused on access and authorization to keep data secure by making sure users follow established policies to control & manage assets

IAM

reduce risk to systems
&
data

Components of IAM

- identification (providing username, ID card, Biometric data ...)
- Authentication :- (to prove id by PIN, password ...)
- Authorization (after confirmed level of access which depends on role in organization)
- accountability → monitoring recording of user actions like login attempts etc

Domain 6

Security assessment and testing

focused on conducting security control, testing, collecting and analyzing data, conducting security audits to monitor for risk & threats & ~~to~~ vulnerabilities

Domain 7

security operations

focused on conducting investigations & implementing preventative measures

digital forensic investigations

Date :

Sr. No.

Domain 8

Software development Security

focused on using secure coding practices

development and testing phase

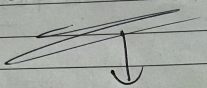
penetration test in deployment and implementation phase

Ransom wave

encrypt data
for money

web layers

Surface web



Deep web

dark web

Key impacts of threats risks, vulnerabilities

Fincal

Identity theft

Reputation

National Institute of Standards & Technology (NIST)

NIST Risk Management framework (RMF)

- prepare
- categorize
- select
- implement
- Assess
- authorize
- Monitor

Steps

Manage security & privacy risk before breach occurs

develop risk management process & tools

2 Choose customize & capture documentation of control that protect an organization

Be aware of how systems are operating

implement security & privacy plans

established controls are implemented correctly

being accountable for security & privacy risks that may exist in an organization

Sr. No.

Date :