Date :
Page No :

## (2/8) Play it Safe : Manage Security Risks

⇒ Course 2 Overview :-

- Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.

① MODULE 1 : Security Domains
↳ CISSP's eight security domains
↳ NIST's RMF

② MODULE 2 : Security frameworks and controls
↳ Security framework & controls
↳ CIA triad
↳ OWASP

③ MODULE 3 : Introduction to Cybersecurity tools
↳ SIEM tools
↳ SIEM dashboards

④ MODULE 4 : Use playbooks to respond to incidents
↳ Playbooks
↳ Respond to identified threats, risks & vulnerabilities

# MODULE 1 :

## CISSP security domains :-

* **Security Posture :-**
An organization's ability to manage its defense of critical assets and data and react to change.

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

### 1. Security and Risk Management :- (focused on)

- Security Goals and Objectives
- (i) • Risk Mitigation
  - Compliance
- (ii) • Business Continuity
  - Legal Regulations

**(i) Risk Mitigation :**
The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach.

Date :
Page No :

(ii) Business Continuity :-

An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

(2) Asset Security : (focused on)

- Securing Digital and Physical Assets
  - Storage
  - Maintenance
  - Retention
  - Destruction of Data

(3) Security Architecture and Engineering :- (focused on)

- Optimizing data security by ensuring effective tools, systems and processes are in place to protect an organization's assets and data

* Shared Responsibility:

All individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security.

(4) Communication and Network Security :- (focused on)

- Managing and Securing Physical networks and wireless communications.

PTO

⑤ Identity and Access Management: (focused on)
- Access and Authorization to keep data secure, ~~secure~~ by making sure users follow established policies to control and manage assets.

* Components of IAM :-
- Identification
- Authentication
- Authorization
- Accountability

⑥ ~~Security Assessment and Testing~~ :

⑥ Security Assessment and Testing : (focused on)
- Conducting Security Control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats and vulnerabilities.

⑦ Security Operations :- (focused on)
- Conducting investigations and implementing preventative measures.

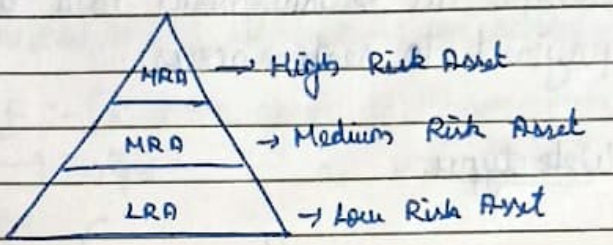
⑧ Software Development Security : (focused on)
- Secure Coding Practices

Date:
Page No:

## ↦ Navigate threats, risks and vulnerabilities :-

- **Threat :**
  Any circumstance or event that can negatively impact assets.

- **Risk :**
  Anything that can impact the CIA triad of an asset.
  ↗ Confidentiality, Integrity, Availability




* **Low-risk Asset :-**
Information that would not harm if the organization's reputation or ongoing operations and would not cause financial damage if compromised.
↳ contents on website ....etc

* **Medium-risk Asset :-**
Information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations.
↳ early release of a quarterly statement

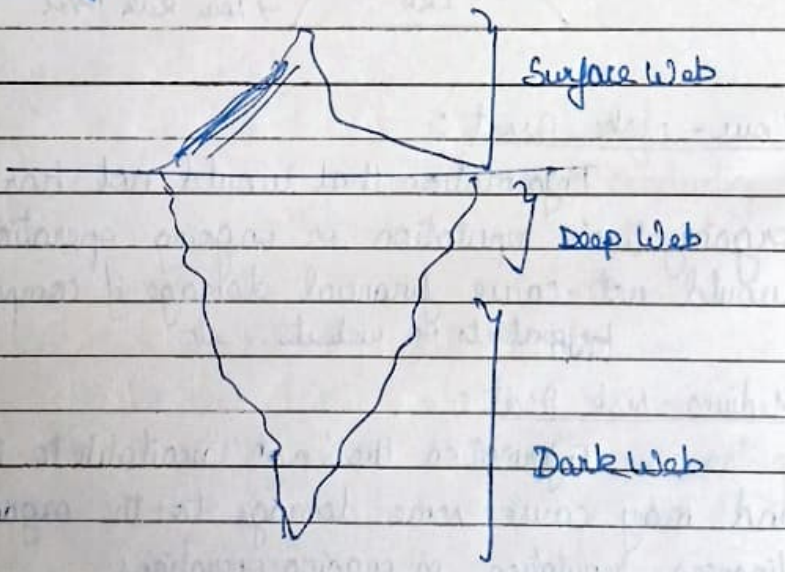
* **High-risk Asset :-**
Information protected by regulations or laws, which if compromised would have a severe negative impact on an organization's finances, ongoing operations, or reputations.
↳ leaked assets with SPII, PII, etc

Date:
Page No:

- **Vulnerability :-**
  A weakness that can be exploited by a threat.
  ↳ outdated firewall, ...etc

⇒ **Ransomware :**
A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

⇒ **Web types:**



Learn to mitigate and manage risks sets yourself apart from other candidates

Date:

⇒ Key Impacts of Threats, Risks & Vulnerabilities:

(i) Financial Impact
(ii) Identity Theft
(iii) Reputation

⇒ NIST: [National Institute of Standards and Technology]
↳ Provides many frameworks for security purposes.

- NIST RMF :- [Risk Management Framework]
↳ 7 steps

(1) Prepare
(2) Categorize
(3) Select
(4) Implement
(5) Assess
(6) Authorize
(7) Monitor

step (1) Prepare:
Activities that are necessary to manage security and privacy risks before a breach occurs

step (2) Categorize:
Used to develop risk management processes and tasks.

step (3) Select:
Choose, customize, and capture documentation of the controls that protect an organization

(4) Implement:
Implement security and privacy plans for the organizations.

(5) Assess:
Determine if established controls are implemented correctly.

(6) Authorize:
Being accountable for the security and privacy risks that may exist in an organization

(7) Monitor:
Be aware of how systems are operating.

---

- APT's: [Advanced Persistent Threats]
A threat actor maintains unauthorized access to a system for an extended period of time.

Date :
Page No :

=> Some Vulnerabilities :

(i) ProxyLogon
(ii) ZeroLogon
(iii) Log4Shell
(iv) PetitPotam
(v) Security logging and monitoring failures
(vi) Server-side request forgery

} learn about them

Date :
Page No :

# MODULE - 2 :-

## Security frameworks and controls

⇒ Security Frameworks:

Guidelines used for building plans to help mitigate risk and threats to data and privacy.

⇒ Security Controls :

Safeguards designed To reduce specific security risks.

(i) Encryption
(ii) Authentication
(iii) Authorization

(i) Encryption:-

The process of converting data from a readable format to an encoded format.

(ii) Authentication:

The process of verifying who someone or something is.

(iii) Authorization:

The concept of granting access to specific resources within a system.

- Cyber Threat Framework [CTF]
- (ISO/IEC) 27001

Date :
Page No :

## The CIA triad : Confidentiality, Integrity and Availability

⇒ **Confidentiality:**
Only authorized users 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.

## NIST frameworks:

⇒ **NIST Cybersecurity Framework : [NIST CSF]**

A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

① ↳ Identify
② ↳ Protect
③ ↳ Detect
④ ↳ Respond
⑤ ↳ Recover

- **NIST S.P. 800-53**
A unified framework for protecting the security of information systems within the federal government.

Date:
Page No:

① Identify:
The management of cybersecurity and its effect on an organization's people and assets.

② Protect:
The strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cysec threats.

③ Detect:
Identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.

④ Respond:
Making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

⑤ Recover:
The process of returning affected systems back to normal operations.

Date :
Page No :

## OWASP principles and security audits :

- OWASP - Open Web Applications Security Project

⇒ OWASP security principles :

(i) Minimize the attack surface area
(ii) Principle of least privilege.
(iii) Defense in depth.
(iv) Separation of duties.
(v) Keep securities simple.
(vi) Fix security issues correctly.

- Additional OWASP security principles :

(vii) Establish secure defaults
(viii) Fail securely
(ix) Don't Trust services (Eg. yone)
(x) ~~Avoid~~
(xi) Avoid security by obscurity

⇒ SECURITY AUDITS :

A review of an organization's security controls, policies, and procedures against a set of expectations.

(i) External
(ii) Internal ⊗ → for entry-level analysts

- Purpose of internal security audits :-
  - Identify organizational risk
  - Assess controls
  - Correct compliance issues

⇒ Common elements of internal audits:

(1) • Establishing the scope and goals
(2) • Conducting a risk assessment
(3) • Completing a controls assessment
(4) • Assessing compliance
(5) • Communicating results

(1) Establishing the scope and goals:

• Scope refers to the specific criteria of an internal audits.
• Goals are an outline of the organization security objectives.

(2) Conducting a risk assessment:

• 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 information in the organization's internal network needs more robust controls in place.

Date :
Page No :

⇒ Audit questions :-

(i) What is the audit meant to achieve?

(ii) Which assets are most at risk?

(iii) Are current controls sufficient to protect those assets?

(iv) What controls and compliance regulations need to be implemented?

(3) Completing a Controls Assessment :-

- Control Categories :
  - Administrative controls
  - Technical controls (hardware/software)
  - Physical controls -

(4) Assessing Compliance :

- Compliance Checklist → must be followed and implemented

(5) Communicating results :

- Stakeholders communications :
  - * Summarizes ~~and~~ scope and goals
  - * Lists existing risks
  - * Notes how quickly those risks need to be addressed
  - * Identifies compliance regulations
  - * Provides recommendations

Date :
Page No :

# MODULE - 3

## Security Information and Event Management dashboards, SIEM dashboards:

→ **Log:**
A record of events that occur within an organization's events and networks.
(i) Firewall logs
(ii) Network logs
(iii) Server logs

(i) **Firewall logs:**
It is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

(ii) **Network logs:-**
It is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

(iii) **Server logs:**
It is a record of events related to services, such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

Date :
Page No :

⇒ SIEM tools:
An application that collects and analyzes log data to monitor critical activities in an organization

• Metrics:
Key technical attributes, such as response time, availability, and failure rate, which are used to assess the performance of a software application.

➡ Explore SIEM tools:-

⇒ Different types of SIEM tools :-

(i) Self - Hosted
(ii) Cloud - Hosted
(iii) Hybrid - combination of both (i) & (ii)

• Examples of SIEM-tools:
(i) * Splunk Enterprise
(ii) * Splunk Cloud
(iii) * Chronicle

(i) Splunk Enterprise :-
A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time.

(ii) Splunk-Cloud:
A cloud-hosted tool used to collect, search and monitor log data.

vii) Chronicle: (google)
A cloud-native tool designed to retain, analyze and search data.

⇒ Open-source tools → Linux, Suricata
⇒ Proprietary tools → Splunk, Chronicle

⇒ Splunk Dashboards:
(1) Security posture dashboard
(2) Executive summary dashboard
(3) Incident review dashboard
(4) Risk analysis dashboard

⇒ Chronicle Dashboards:
(1) Enterprise insight dashboard
(2) Data ingestion and health dashboard
(3) IOC matches dashboard (Indicators of compromise)
(4) Main dashboard
(5) Rule detection dashboard
(6) User sign in dashboard overview

Soft skills >> technical skills.

Date :
Page No :

## MODULE - 4 :-

## Use of playbooks to respond to incidents :-

⇒ **Playbook:**
A manual that provides details about any operational action.

⇒ **Incident response:**
An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach.

⇒ **Incident response playbook : (6 phases)**

(1) Preparation
(2) Detection and analysis
(3) Containment
(4) Eradication and Recovery
(5) Post incident activity
(6) Coordination

## Explore Incident response :-

simple points

— × —— ×—