2015-0247
Insha Sammani
BSCS-7E

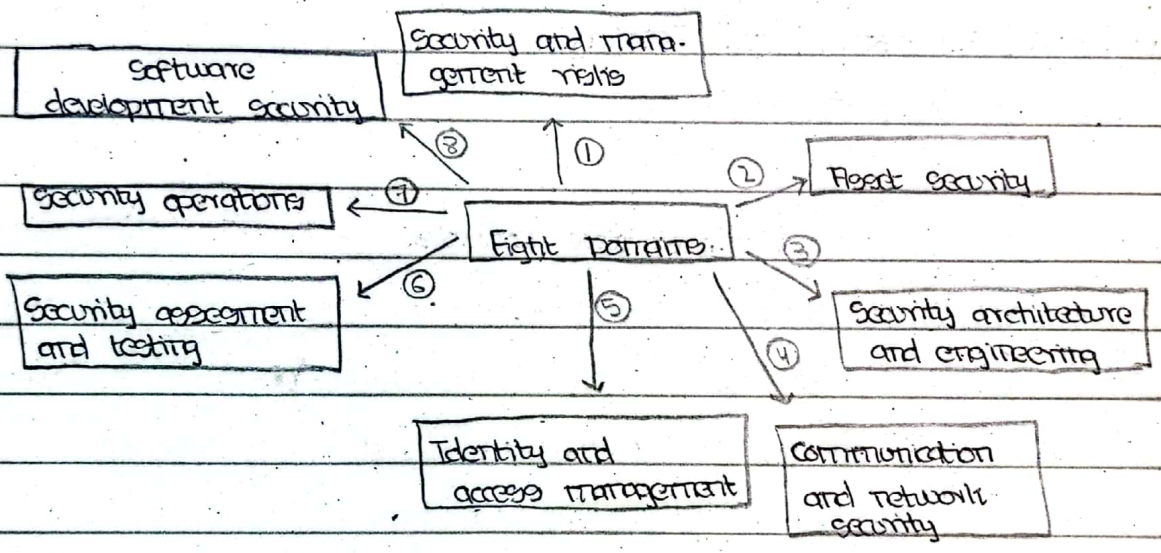
HOW TO MANAGE SECURITY RISKS AND THREATS

Date

Security Domains Overview:

CISSP ki saath security domains ka introduction.

- Security domains, frameworks aur controls ka in-depth coverage, specially NIST ka RMF pe focus.
- Security audits ki exploration, including internal audit elements.
- Introduction to basic security tools and their use.



Security Domains: 1. Security and Risk Management:

- Purpose: Security goals, Risk mitigation, compliance, Business continuity, legal regulations.

2. Asset Security:

- Focus: Digital or physical asset ki, data storage, maintainance, retention, and security destruction.

3. Security Architecture and Engineering:

- Focus: Data security, to optimize karne ki liye effective tools, systems, or processes.

Scanned with CamScanner

Date

4. Communication and Network Security:

- Focus: Physical networks or wireless communications to manage or secure data.

5. Identity and Access Management:

- Components: Identification, authentication, authorization, accountability.

6. Security Assessment and Testing:

- Focus: Security control testing, data analysis, air security audits conduct data.

Administrative Controls			
Control name	Control type and explanation	Need to be implemented	Priority
Password Policies	Preventative; establish password strength rules to improve security/ reduce likelihood of account compromise through brute force or dictionary attack techniques.	X	High

Technical Controls			
Intrusion Detection System (IDS)	Detective; allow IT teams to detect possible intrusions (; anomalous traffic) quickly.	X	High
Encryption	Deterrent; makes confidential information/data more secure (i.e website payment transactions)	X	High

Scanned with CamScanner

Date

Physical controls			
Control Name	Control Type and Application	Needs to be Implemented	Priority
Closed Circuit television (CCTV)	preventive/detective; can reduce risk of certain events; can be used after event for investigation	X	High
locks	Preventive; physical and digital assets are more secure.	X	High

7. **Security Operations:**

- Focus: Investigations, preventive measures implement karna, forensic investigations conduct karna.

8. **Software Development Security:**

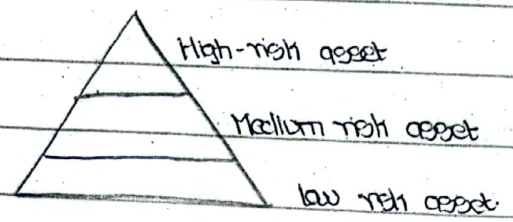
- Focus: Securing coding practices use karna throughout SDLC.

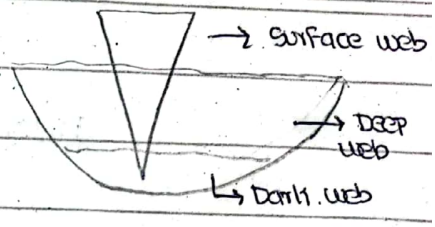
Threats, Risks, and Vulnerabilities:

- Threats: circumstances ya events jo assets ko negative way mai use karte hain. Example: Social engineering attacks, phishing.
- Risks: Confidentality, Integrity ya Availability ko impact karne wale kuch bhi. levels (low, medium, High) mai rate hota hai.
- Vulnerabilities: Threats exploit kiye jaa sakte hain. Example: Outdated firewall, weak passwords, un protected data. Vulnerabilities ko manage karne ki liye education and empowerment zaroori hai. Entry-level analyst ka role hai begin ko security conscious banane mai.

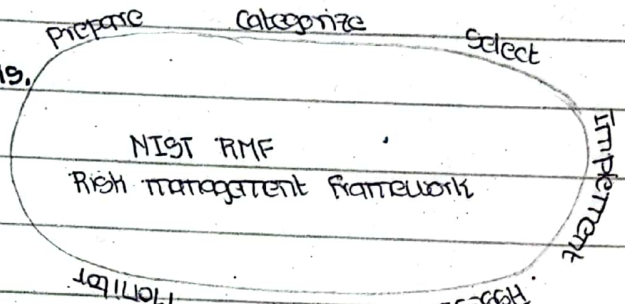
Scanned with CamScanner

Date





Impacts of Threats, Risks, and Vulnerabilities:

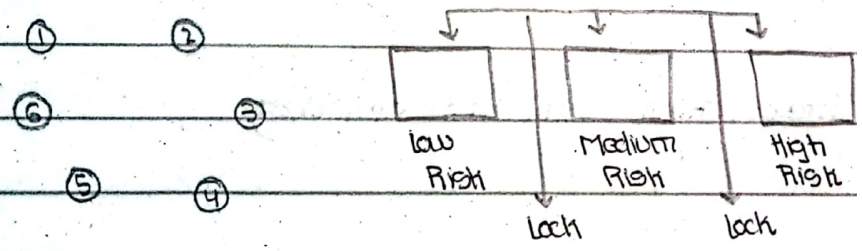


Ransomware:

- Malicious attack jo data ko encrypt karta hai aur access restore k liye payment mangta hai.
- Organizational operations par been key impacts. Financial impact, Identity theft, reputation damage.

NIST Risk Management Framework:

- Seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor.



Review of Course Section:

- CISSP ke saath security domains, threats, risks, vulnerabilities, ransomware, aur web ki 3 layers ko cover kia hai.
- NIST RMF ke 7 steps ko manage karne ki importance.
- Entry-level analysts ki security maintain karne mai importance.

Introduction to Security Frameworks and Controls:

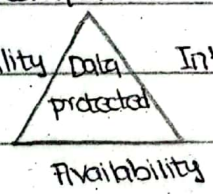
Scanned with CamScanner

Date

- Security frameworks guidelines tote tain risks mitigate or plans banane ke liye.
- Overlapping requirements jo organizations aur logon ko protect karne ke liye use.
- Frameworks security policies aur processes banane ke liye starting point provide karte tain.

Security Controls:

- Safeguards jo specific security risks ko kam karne ke liye design kiye gaye tote tain. • Common types: Encryption, Authentication, Authorization.
- CIA Triad: core security model ke components - Confidentiality, Integrity, Availability.



Security Tools- Logs:

- Logs events ki record tote tain organization ke systems aur networks mai.
- Common log sources: firewall logs, network logs, server logs.
- Logs ko monitor karna vulnerabilities aur potential breaches ko identify karne mai help karta tai.

Security Information and Event Management (SIEM) Tools:

- SIEM tools log data collect aur analyze karte tain.
- Provide real-time visibility, event monitoring, automated alerts, aur centralized log storage.
- Efficiency bartane ke liye logs ko index aur minimize karte tain.

SIEM Dashboards:

Scanned with CamScanner

Date

- Dashboards information ko visual form mai present karte hain for quick understandi bility
- Weather apps ki tarha, SIEM dashboards security analysts ko informed decisions lene mai help karte hai.
- Charts, graphs, tables se security information ko summarize karte hain.

Example Scenario - SIEM Dashboard Use:

- Analyst ko alert milta hai suspicious login attempt ka.
- SIEM dashboard access karta hai information gather karne ki liye.
- Unusual login locations aur times ko identify karta hai.
- Dashboard ki visual representation quick analysis mai help karte hain.

Metrics in SIEM Dashboards:

- Dashboards stakeholders ko metrics provide karte hain.
- Metrics software applications ki performance assess karne ki liye use hota hai
- Customizable dashboards diff organizational members ki liye relevant metrics display kar skte hain.

Types of SIEM Tools:

- Self hosted SIEM tools: Organization ki aur physical infrastructure se installed, operated, aur maintained hote hain.
- Cloud hosted SIEM tools: Third party vendors ko maintain or manage karta, accessible through internet.
- Hybrid solution: Self hosted or cloud hosted SIEM tools ka combination.

Common SIEM Tools:

RC.

Scanned with CamScanner

Date

- Splunk enterprise: self hosted tools for data analysis, real-time alerts, aur necessary information ki liye.
- Splunk cloud: cloud hosted tools for data collection, searching and monitoring.
- Chronicle (by Google): cloud native tools for monitoring, data analysis and data collection.

Purpose of Playbooks:

- Playbooks manuals hote hain jo manual operations dictate karte hain security incidents ki response mai.
- Provides structure, ensure compliance, aur documentation aur communication ki liye processes guide karte hain.

Incident Response Playbook:

- Six phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity, Coordination.
- Playbooks security analysts ko guide karte hain ek consistent process mai security incidents ki response mai.

Usage of Incident Response Playbook:

- Examples include malware attacks, phishing actions assessment, containment, eradication, aur recovery ki liye define kiye hote hain.
- Playbooks living documents hote hain, jo lessons learned aur evolving threats ki basis par update kiye jate hain.

Importance of Playbooks for Security Analysts:

RC

Scanned with CamScanner

Date

- Security teams frequent updates karti hain playbooks ko address karne k liye for new threats and vulnerabilities.
- Entry-level analysts ko playbooks frequent use mai help karte hain, especially incident response mai.

Recap and Summary:

- Importance of logs in cyber security.
- Introduction of SIEM Dashboards and common SIEM tools.
- Playbooks and their roles in incident response and its significance.
- Overview of CISSP and its domains.
- Exploration of threats, risks and vulnerabilities.
- Discussion for security frameworks, controls, and principles.
- Relationships between frameworks, control, and security audits.
- Basic security tools like SIEM dashboards and playbooks.

Scanned with CamScanner

2011-0247
Insha Sammani
BSCS-7E

RISK MANAGEMENT FRAMEWORK (RMF)

Introduction:

- IMF ka high level overview.
- Mostly used by department of defence aur US government.
- NIST 800-37 ke mutabiq defined hai jisha latest version hai V2.

Real World Examples:

- How to use RMF in different situations. To prove this, include real world examples or case studies so that it could be easy for viewers to understand.

Introduction of Terms:

CIA triad, NIST, aur RMF ka small introduction or details include karein so that viewers wo don't know abbreviations can understand.

Framework Overview:

- Seven steps including preparation.
- Not a regulation but a framework with varied implementations.
- Used differently by different defence organizations.

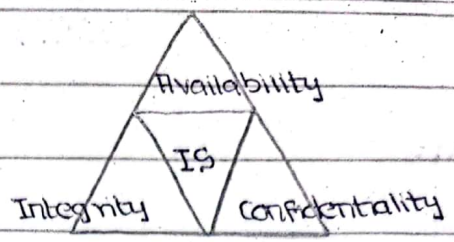
Step 1: Categorize Information System:

- Based on CIA triad: Confidentiality, Integrity, Availability.
- Inputs: Architecture description, organizational inputs.
- Security category assigned per information type or system.
- Security objectives: Confidentiality, Integrity, Availability.
- Impact values: Low, Moderate, High.
- Security Category (SC) information type/system = (confidentiality, x), (Int-

Scanned with CamScanner

Date

egrity, x), (availability, x).



Information Types:

- Specific category of information (eg privacy, medical, proprietary, financial, investigation, contractor-sensitive, security management), defined by an organizer or;
- A public law, executive order, directive, policy, or regulation.

Example: Security Category $(SC)_{PHI}$ = (Confidentiality, High), (Integrity, High), (Availability, Low).

Step 2: Select Controls:

- Based on categorization.
- Use NIST 800-53, latest revision is 5.
- Consider tailoring control based on risk or local conditions.

Step 3: Implement Controls:

- Document the implementation process.

Step 4: Access Controls:

- Use NIST 800-53 as a guide.
- Examine, interview and test controls.
- Artifacts needed for control substantiation.

Step 5: Authorize Information System:

- Decision to authorize the system.
- Formal acceptance or risk by an authorized entity.

Scanned with CamScanner

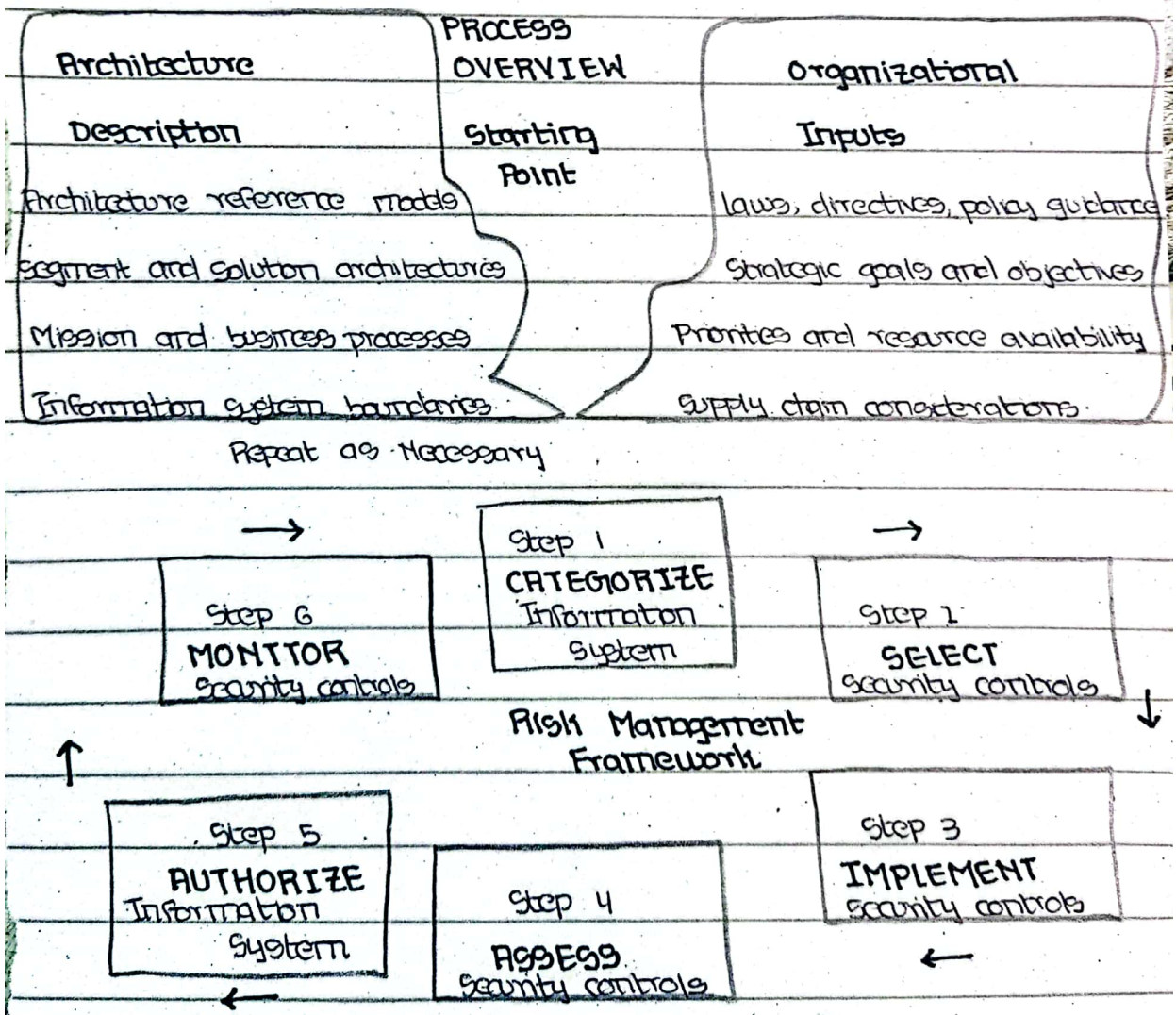
Date

Step 6: Monitor Controls:

- Continuos monitoring of security controls.
- Risks, environments, and likelihood of exploits change.
- Suggested more frequent monitoring, atleast anually.

Importance of Every Step:

- Highlight importance of every step of RMF and tell how it contributes to overall risk management and cyber security.



Conclusion And Recap:

Scanned with CamScanner

Date

- Details of steps.
- Focus on changing of the steps.
- Focus on specific class of risk management framework.

Challenges and Considerations:

- Briefly discuss potential challenges or considerations that organization might face during the RMF process implementation.

Resources and References:

Provide additional resources or references for viewers who want to delve deeper into RMF or related topics.

Scanned with CamScanner

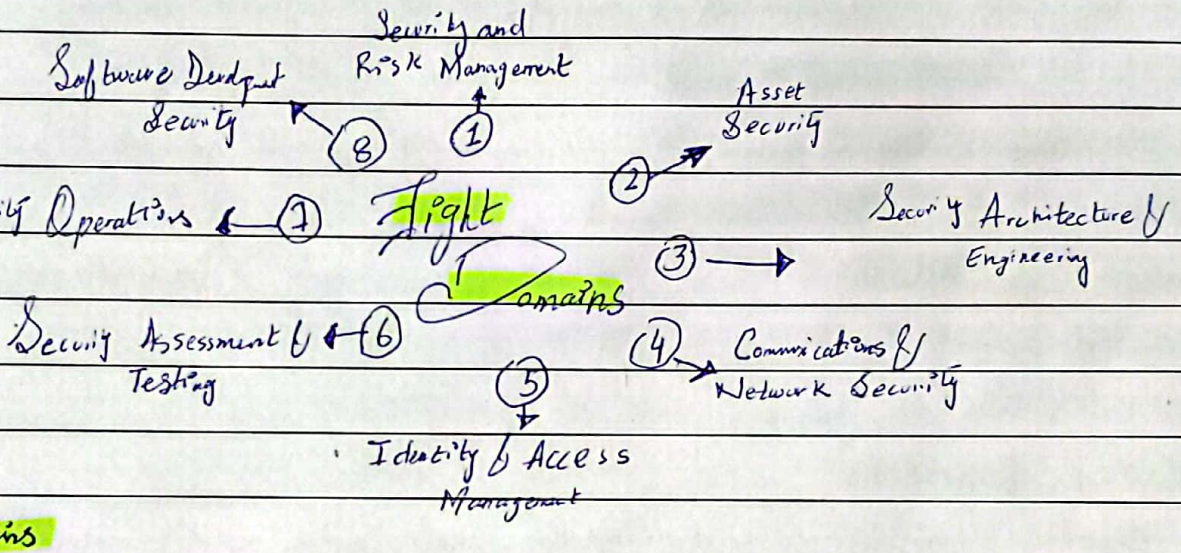
HOW TO MANAGE SECURITY RISKS & THREATS

Ismail Ansari
20K0228
BSCS-7E

Date _____

Security Domains Overview:

In this section, we provided an in-depth exploration of the fundamental components within CISSP eight security domains. These domains cover security and risk management, asset security, security architecture & engineering, communication & network security, identity & access management, security assessment & testing, security operations & software development security.



Security Domains

1. **Security & Risk Management** :- Covering areas such as security goals, risk mitigation, compliance, business continuity & legal regulations.
2. **Asset Security** :- Focusing on the protection of digital & physical assets, including data storage, maintenance, retention & destruction
3. **Security Architecture & Engineering** :- Centered on optimizing data security through effective tools systems & processes
4. **Communication & Network Security** :- Concentrating on the management & securing of physical networks and wireless communications.
5. **Identity & Access Management (IAM)** :- Involving components like identification, authentication, authorization & accountability
6. **Security Assessment & Testing** :- Emphasizing the conduct of security control testing, data analysis, and security audits.

Scanned with CamScanner

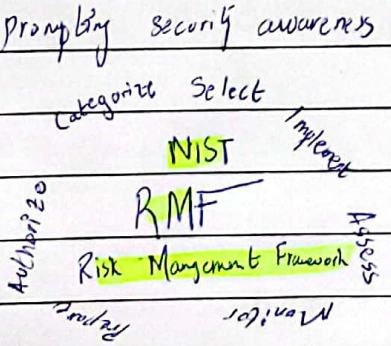
Control Name	Control Type and Explanation	Needs to be Implemented (X)	Priority
	Administrative Controls		
Password Policies	Preventative, establish password strength rules to improve security / reduce likelihood of account compromise through brute force or dictionary attacks	X	High
	Technical Controls		
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (i.e. anomalous traffic) quickly	X	High
Encryption	Deterrent; makes confidential information/data more secure (i.e. website payment transactions)	X	High
	Physical Controls		
Closed-Circuit Television (CCTV) surveillence	Preventative / Detective; can reduce risk of certain events, can be used for after event investigation	X	High
Locks	Preventative; physical & digital assets are more secure	X	High

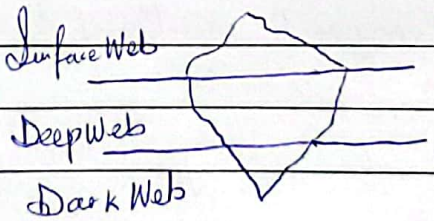
7. Security Operations :- With a focus investigations, implementing preventive measures, and conducting forensic investigations.

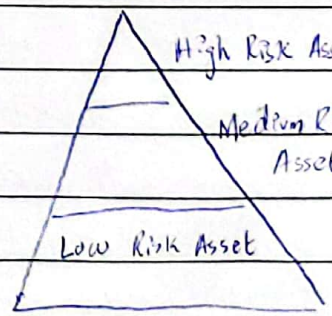
8. Software Development Security - Highlighting the use of secure coding practices throughout the software development life cycle

Threats, Risks & Vulnerabilities :-

Examining threats as circumstances negatively impacting assets, risks affecting confidentiality, integrity, or availability, and vulnerabilities as weaknesses exploitable by threats. Emphasizing the role of education and empowerment in managing vulnerabilities, with entry-level analysts playing a crucial role in prompting security awareness







Impacts of Threats, Risks & Vulnerabilities :-

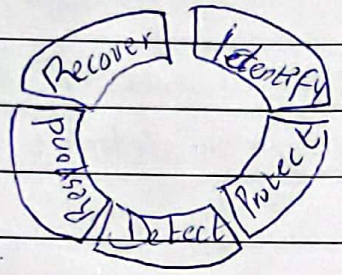
Exploring the malicious impacts of ransomware on organizational operations, including financial consequences, identity theft and reputation damage.

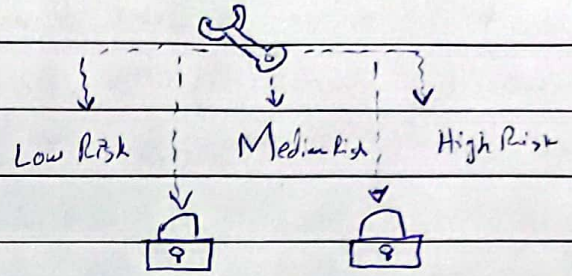
Scanned with CamScanner

Date_____

NIST Risk Management Framework (RMF)

A review of the 7-step NIST RMF Process: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor, underscoring its importance in effective risk management.





Review of Course Sections:

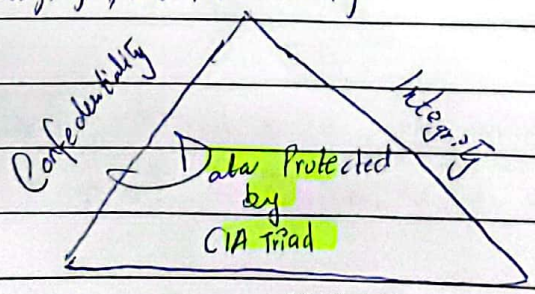
Summarizing the coverage of CISSP's eight security domains, threats, risks, vulnerabilities, ransomware, and the layers of the web. Highlighting the significance of the NIST RMF's 7 steps & the crucial role of entry-level analysts in maintaining security.

Introduction to Security Frameworks & Controls:

Exploring the security frameworks as guidelines for risk mitigation plans, their overlapping requirements for protecting organizations & individuals, and their role as a starting point for creating security policies & processes.

Security Controls:

Defining safeguards designed to reduce specific security risks, with common types including encryption, authentication and authorization. Introducing the CIA Triad as the core components of the security model: Confidentiality, Integrity, and Availability.



Al Habib

Scanned with CamScanner

Date

Security Tools ~~[illegible]~~.

1. Logs: Examining logs as records of events in organizational systems & networks, with common sources being firewall logs, network logs, and server logs. Emphasizing the role of monitoring logs in identifying vulnerabilities & potential breaches.
2. Security Information & Event Management (SIEM) Tools.. Introducing SIEM Tools that collects and analyze log data, providing real-time visibility, event monitoring, automated alerts, and centralized log storage. Emphasizing the efficiency gained through indexing & minimizing log

SIEM Dashboards.

Describing SIEM dashboards as visual tools for quick understanding, similar to weather apps, Emphasizing their role in assisting security analysts in making informed decisions by presenting security information in charts, graphs, or tables.

Example Scenario - SIEM Dashboard Use:

Illustrating the use of SIEM dashboards as in a practical scenario, where an analyst receives an alert about a suspicious login attempt, access the dashboard, and quickly identifies unusual login patterns through visual representations.

Metrics in SIEM Dashboards.

Highlighting the role of dashboards in providing stakeholders with metrics, key technical attributes used to assess software application performance. Emphasizing the customization of dashboards to display relevant metrics for different organizational members.

Types of SIEM Tools..

Differentiating b/w self-hosted SIEM tools, cloud-hosted SIEM tools, and hybrid solutions. Mentioning common SIEM tools such as Splunk Enterprise, Splunk Cloud, and Chronicle (by Google).

Scanned with CamScanner

Date

Purpose of Playbooks:-

Defining playbooks as manuals detailing operational actions in response to security incidents. Emphasizing their role in providing structure, ensuring compliance, and guiding processes for communication & documentation

Incident Response Playbook:-

Outlining the six phases of an incident response playbook: Preparation, Detection and Analysis Containment, Eradication & Recovery, Post-Incident Activity, and Coordination. Emphasizing how playbooks guide security analysts through a consistent process in responding to security incidents.

Usage of Incident Response Playbook:-

Examining the practical application of incident response playbooks in guiding security analysts through consistent processes, using example like addressing malware attacks with defined actions for assessment, containment, eradication, and recovery. Highlighting playbooks as living documents updated based on lessons learned & evolving threats.

Importance of Playbooks for Security Analysts:-

Stressing the significance of playbooks in providing a structured and consistent approach to responding to incidents. Emphasizing that security teams frequently update playbooks to address new threats and vulnerabilities, with entry-level analysts playing a crucial role, especially in incident response.

Scanned with CamScanner

- Ismail Ansari
2020228
BCS-7E

RISK MANAGEMENT FRAMEWORK (RMF)

Date_____

Introduction

The Risk Management Framework (RMF) provides a high-level overview, primarily employed by the Department of Defense and the US Government. Defined according to NIST 800-37, its latest version is version two.

Real-world Examples:

To demonstrate the varied applications of RMF in different settings, real-world examples and case studies are included, aiming to make it easily understandable for viewers

Introduction to Terms:

A concise introduction or detailed explaination of terms such as the CIA Triad, NIST, and RMF is provided to ensure that viewers unfamiliar with these abbreviations can comprehend their significance

Framework Overview:

The framework consists of 7 steps, including prepration. It is not a regulation but a flexible framework with diverse implementations, tailored differently by various defense organizations.

Step1: (Categorize Information System)

Based on the CIA triad (Confidentiality, Integrity, Availability), this step involves categorizing the information system. Input include architechture descriptions and organizational Inputs, & security categories are assigned based on information types or systems.

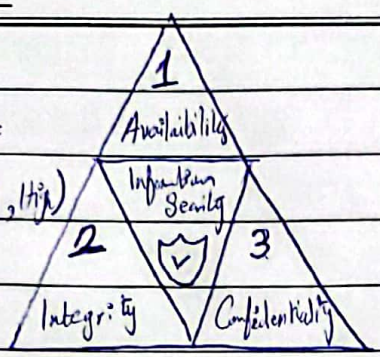
Scanned with CamScanner

Date

Example:

Security Category (SC) =

(confidentiality, High), (Integrity, High)
(availability, Low)



Information Types

- Specific category of information (eg privacy, medical, proprietary, financial, investigate, contractor-sensitive, security management) defined by an organization or;
- A public law, executive order, directive, policy or regulation

Step 2: (Select Controls)

Building on the categorization, controls are selected using NIST 800-53. Tailoring controls based on risk or local conditions is considered.

Step 3: (Implement Controls)

The implementation process is documented during this step.

Step 4: (Assess Controls)

Using NIST 800-53 as a guide, controls are examined, interviewed, and tested. Artifacts are necessary for control substantiation.

Step 5: (Authorize Information System)

This step involves making the decision to authorize the system, formalizing the acceptance of risk by an authorized entity

Step 6: (Monitor Controls)

Continous monitoring of security controls is crucial as risks, environments, and the likelihood of exploits change. More frequent monitoring, at least annually, is recommended.

Importance of Each Step..

The script emphasizes the significance of each step in RMF, highlighting how they contribute to overall risk management & cybersecurity.

Al Habib

Scanned with CamScanner

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes Information
System Boundaries.

Date _____

PROCESS OVERVIEW
Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals & Objectives Priorities
Priorities and Resource Availability
Supply Chain considerations

Report on necessary

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

RISK MANAGEMENT FRAMEWORK

Conclusion & Recap:

A recap of the steps is provided, emphasizing the need to address changing risks and signaling a reflective stance towards the Risk Management Framework.

Challenges & Considerations.

Briefly discussing potential challenges or considerations during the RMF implementation process acknowledges the complexities organizations might face.

Resources & References:

Additional resources or references are provided for viewers interested in diving deeper into RMF or related topics.

Closing:

Encouragement is extended for questions, comments, and suggestions. A subscription request for the channel is made, and a link to the Certified Authorization Professional Class is provided.

Scanned with CamScanner

20K-0207
E
Yusra Adam

Video → How To Manage Security Risks and Threats

Security Domains → 8 security domains by CISSP (certified information systems security professionals)

1- Security and risk management :- It deals with security goals, risk mitigation, compliance, business continuity and legal regulations. Examples include PII protection, risk procedures, compliance for internal security policies

2- Asset Security Domain :- It focuses on securing digital & physical assets. Importance of policies for data handling and protection. Examples include data disposal, overseeing destruction of hard drives.

3- Security Architecture and engineering domain:- It focuses on optimizing data security through effective tools and shared responsibility. Examples include policies promoting user involvement in security.

4- Communication and network security domain:- It focuses on managing and securing physical networks and wireless communications. Examples include protecting remote employees from insecure connections.

5- Identity and access Management (IAM):- It focuses on accessing and authorization, reducing overall risk.

Components

- Identification
- Authentication
- Authorization
- Accountability

Scanned with CamScanner

6- Security Assessment and Testing:- It focuses on security control testing, data analysis and audits. Examples include multi-factor authentication implementation.

7- Security Operations:- Focuses on investigations, preventative measures and forensic analysis. Examples include neutralizing threats, digital and physical evidence collection.

8- Software development Security :- It focuses on securing coding practices in the SDLC. Incorporating security at each phase to ensure data protection. Examples include secure design reviews, code reviews, penetration testing.

Security Threats, Risks & Vulnerabilities → Security analyst job is to protect organization's assets.

Assets (item perceived as having any value)

- physical office spaces
- Computers
- intellectual property (IP)
- Patents & copyrighted data

Threat :- any event that negatively impact organization's assets. Example :- social engineering attack (exploits human error to gain private and secret information)

Phishing :- technique used to acquire sensitive data such as usernames, passwords or banking information.

Risk :- compromise on CIA (confidentiality, integrity or availability) of an asset.

Scanned with CamScanner

*PII → personal identifiable information

Risks

- Low (dont harm organization's assets)
  - public info such as website content
- Medium (cause damage to organization)
  - early release of company's quarterly earnings.
- High (protected by laws & regulations).
  - Leaked assets with SPII, PII, IP.

Vulnerabilities :- weakness that can be exploited by a threat. Examples include outdated firewall, weak passwords, unprotected confidential data.

Web Layers → Three Layers
- Surface web
- Deep web
- Dark web

1) Surface Web → most people use. Contains content that is accessible by web browser.

2) Deep Web → requires authorization to access it. Example is of intranet bcz it is only accessible by employees or others who have been granted access.

3) Dark Web → negative connotation bcz of its association with criminal activities. Criminals prefers dark web for secrecy.

Impacts of Threats, Risks & Vulnerabilities → 3 Key impacts :-
- Financial impact
- Identity Theft
- Damage To Reputation

Scanned with CamScanner

1- Financial Impact :- It involves significant financial loses due to comprimised assets. The reasons behind this are interrupted production, corrective costs, fines for non-compliance with laws. Example include malware attack affecting operations.

2- Identity Theft :- Is me customer aur employees ka private data store karnay. Storing private and sensitive data possess risk. Dark web provides secrecy for selling data without legal consequences.

3- Damage To Reputation :- Solid customer base support an organization's missions and financial goals. Exploited vulnerabilities lead to customers seeking new business relationships.

Risk Management Framework (RMF) → RMF provides steps for managing risks, threats and vulnerabilities.

RMF Steps

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

1) Prepare :- Isme breach se pehle jo activities honi chahiye woh aati to manage security & privacy risks.

2) Categorize :- Developing risk management processes by considering CIA triad.

3) Select :- Choosing, customizing and documenting controls.

4) Implement :- Executing security and privacy plans to

Scanned with CamScanner

minimize ongoing risks.

5- Assess :- To determinie whether the implementations done in previous step are upto mark or not.

6- Authorize :- Being accountable for security and privacy risks. It involves generating reports.

7- Monitor :- Being aware of system operations. Ensuring system supports security goals.

CIA Triad → Confidentiality, Integrity & Availability

Confidentiality	Integrity	Availability
• Only authorized users access specific aset.	Data is correct, authentic & reliable.	Data is accessible t authorized users.
Example → banks safeguards personal & financial information.	Example → Banks verifying account activity for authenticity.	- Example → banks ensure account inf is accessible Onlin

Cyber Security Framework (CSF) → Developing plans to mitigate risks. Framework for managing cyber security risks.

Core Functions

- Identify
- Protect
- Detect
- Respond
- Recover

Scanned with CamScanner

*MFA → multi factor authentication

1) Identify :- Manage cybersecurity risk and its impact. Example include monitoring internal network for potential security issues.

2) Protect :- Strategy using policies, procedures, trainings. Examples include improving policies and procedures base on historical data.

3) Detect :- Identify potential security incidents and improve monitoring. Examples include reviewing new security tools.

4) Respond :- Contain, neutralize, analyze security incidents, implement improvement.

5) Recover :- return affected systems to normal operation. Examples include restoring systems and data after a breach.

Open Web Application Security Project (OWASP) → Some principles of OWASP are discussed below :-

- Minimizing Attack surface area :- Reducing potential vulnerabilities. Examples include disabling unnecessary software features.
- Principle of least privilege :- Users have been given the least access required. Example include limiting user access to prevent misuse.
- Defense in Depth :- multiple security controls addressing risks. Example include MFA.

Scanned with CamScanner

-Separation of duties:- Preventing indivituals from carrying out fraudulent activities.

Security Audits → review of an organization's security against expectations.

Security Audits

Internal | External

Internal Security Audit:- Conducted by team including compliance officer and security manager. Elements of internal security audits are:- Scope & goals, Risk assessment

Underscope & goals and risk assessment we have below elements:-

1- Controls Assessment:- Involves classifying controls into 3 categories:-

Administrative Controls	Technical Controls	Physical Controls
• Pertains to human aspect of cyber security.	• Involves hardware and software solutions.	• Measures to prevent physical access
• Policies and procedures managing data.	• Intrusion detection (IDS), encryption.	• Surveillance cameras & locks

Scanned with CamScanner

2- Compliance Assessment:- To determine if the organization adheres to necessary compliance regulations.
3- Communication:- Final common element which involves audit scope, existing risks, identifying compliance regulations.

Importance of Audits → • Identify gaps in an organization's security measures.
• Guiding improvements for desired security postures.
• Provide immense value to organizations.

Security ~~Management~~ Information and Event Management (SIEM) → Below provides description regarding SIEM tools and logs:-
Log Types:- Security analyst use logs to monitor system.

Log Sources
- Firewall Logs
- Network Logs
- Server Logs

SIEM Dashboards:- Uses visual representation to provide quick & insights to organization's security postures.
Display metrices such as response time and availability,

SIEM Tools → Splunk and Chronicle
- Splunk ↓ self hosted solutions
- Chronicle ↳ cloud-native tool

Scanned with CamScanner

Playbooks → provide structured responses to security incidents. They ensure consistency, compliance and efficiency in addressing threats.

Incident Response Playbook → 6 phases

Phases

- Preparation
- Detection & Analysis
- Containment
- Eradication & Recovery
- Post incident activity

Importance:- Playbooks are living documents frequently updated to address evolving threats. Plays a vital role in organization learning from past incidents to enhance security postures.

Scanned with CamScanner

Video → Risk Management Framework (RMF)

RMF → RMF is comprised of 6 steps :-

1- Categorize the information system :- It is based on 3 tenant of information security, CIA (confidentiality, integrity & availability). Impact values rated as low, moderated or high. Security category assigned for each information system.

Example : Categorization for protected health information

	Confidentiality	Integrity	Availability
Impact values	High	High	Low

2- Selection of controls :- Initial set of baseline controls selected for system. Consideration of tailoring and supplementing based on risk or local conditions.

3- Implement Controls :- Implementation of chosen controls and documentation of implemented controls.

4- Assess Controls :- Assess controls to ensure they are implemented as intended and effective.

5- Authorization of system :- Formal decision to authorize the system to operate in a normal environment.

6- Monitor Controls :- Continuous monitoring of security controls. Risks change and controls need to adapt.

Scanned with CamScanner

Risk Management Framework for Information Systems & Organizations :-

* Due to increase complexity in hardware, software and systems especially in critical infrastructure enlarges attack surface for adversaries.
* Government Initiatives → recognizes increasing interconnections of federal information systems. requires appropriate risk management for both federal agencies.
* Seven major objectives:-

1) Closer Linkage :- Between risk management processes at the governance and operations level.
2) Integration with NIST Cybersecurity framework :- Alignment with NIST cybersecurity framework for effective implementation.
3) Privacy Integration :- Integration of privacy risk management processes into RMF.
4) Secure Software Development :- Promotion of trustworthy secure software and systems.
5) Supply chain Risk Management (SCRM) :- Integration of SCRM concept into RMF.
6) Control Selection Approach :- Introduction of an organization-generated control selection approach.

Scanned with CamScanner

Benefits of Updated RMF:-

- Simplifies RMF execution, promotes consistency and increases automation.
- Maximizes use of common controls, shared systems and organization defined controls.
- Reduces complexity, increases efficiency and promotes ongoing authorization and continuous monitoring.

Scanned with CamScanner