INFORMATION SECURTIY CS-3002

JS BANK THREAT AND RISK ASSESSMENT

PROJECT REPORT

SUBMITTED TO:

Ms. Yusra Kaleem

GROUP MEMBERS:

INSHA SAMNANI **20K-0247**

ISMAIL AHMED ANSARI **20K-0228**

YUSRA ADAM **20K-0207**

70 QUESTIONS AND ANSWERS

FINANCIAL SECTOR (JS BANK)

Introduction:

Established in 2006, JS Bank has evolved significantly since its inception, originating from the acquisition of Citicorp Investment Bank Limited. With a robust presence in both domestic and international markets, the bank has become a dynamic financial institution. Recognized for excellence in digital financial services, SME, and consumer lending, JS Bank, a part of the JS Group, remains dedicated to making a positive impact on the lives of its customers. Committed to a secure financial relationship, the bank emphasizes ongoing efforts to enhance security parameters, acknowledging the prevalent risks in today's digital landscape. In the ever-evolving realm of cyber threats, JS Bank ensures continuous vigilance while providing a safe and secure banking experience for its customers.

Services provided by JS Bank:

1- **Security Measures:**

The advisory assures customers that JS Bank prioritizes the protection of personal information. Multiple layers of security are implemented in both mobile and internet banking services to prevent unauthorized access. Importantly, JS Bank emphasizes that it will never request personal information through email, phone, or SMS.

2- **Highlighting of common Types of Internets and Mobile Banking Fraud:**

JS Bank highlights several common types of fraud, including phishing/scamming, malware and viruses, mobile fraud, and text message fraud (smishing). It emphasizes that fraudsters employ sophisticated tools to deceive users and gain access to financial information.

3- **Customer Tips for Security:**

JS Bank provides customers with practical tips to enhance their information security, including avoiding sharing personal information, creating strong passwords, using secure methods on public computers, and promptly reporting lost or stolen mobile phones.

4- **Security Advisory Contacts:**

Customers are urged to report any suspicious emails, websites, or SMS messages to JS Bank through the dedicated helpline at 0800-011-22.

5- **Privacy Guardian Services:**

5.1- Handling Personal Information: JS Bank respects the privacy of personal information provided by customers. The Privacy Statement outlines the purposes for which the information may be used, including providing requested services, conducting credit checks, and improving services based on customer feedback.

5.2- Information Disclosure: The statement clarifies that customer details may be disclosed to entities within the JS Bank Group, regulatory authorities, service providers, credit reference agencies, and other relevant parties for specified purposes. JS Bank emphasizes secure and confidential treatment of transferred information.

5.3- Cookies and Internet Communications and Web Tracking:

JS Bank occasionally uses cookies to enhance internet services. These cookies help recognize users' interests, enable access to online services, and provide statistical information for website improvement.

5.4- Monitoring Internet Communications:

To maintain system security and prevent unauthorized activities, JS Bank reserves the right to monitor all internet communications, including web and email traffic.

ANSWERS TO 70 QUESTIONS

Q1: Do you conduct robust and frequent end-user cybersecurity awareness training?

A1: Yes, JS Bank conducts regular and comprehensive cybersecurity awareness training programs for end-users to ensure they are well-informed about potential risks and security best practices.

Q2: Have you taught everyone how to securely store passwords or passphrases?

A2: Yes, JS Bank has implemented training sessions to educate staff and customers on secure password practices, emphasizing the importance of strong, unique passwords or passphrases.

Q3: Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?

A3: Yes, JS Bank regularly organizes anti-phishing, smishing, and vishing campaigns to simulate real-world scenarios, assess the readiness of employees and customers, and enhance their ability to recognize and respond to potential threats.

Q4: Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors, and how to report any suspicious activities for further investigation?

A4: Yes, JS Bank ensures that all employees are well-versed in the risks associated with cybersecurity. They are trained to recognize common tactics employed by threat actors and are encouraged to promptly report any suspicious activities for thorough investigation.

Q5: Are all vendor default accounts changed or disabled?

A5: Yes, JS Bank ensures that default accounts from vendors are either changed or disabled to prevent unauthorized access and enhance the overall security of the system.

Q6: Are only necessary services, protocols, daemons, and functions enabled?

A6: Yes, JS Bank employs a strict policy to enable only essential services, protocols, daemons, and functions, minimizing potential vulnerabilities and reducing the attack surface.

Q7: Is all unnecessary functionality removed or disabled?

A7: Yes, JS Bank takes measures to remove or disable any unnecessary functionality, reducing the complexity of the system and mitigating the risk of potential security breaches.

Q8: Are all accounts immediately disabled or deleted upon termination of employment?

A8: Yes, JS Bank follows a robust account management process, ensuring that accounts are promptly disabled or deleted when an employee's tenure terminates, preventing unauthorized access.

Q9: Are all screen idle times set for 15 minutes, and do they require re-authentication to unlock?

A9: Yes, JS Bank enforces a security policy where screen idle times are set to 15 minutes, and re-authentication is required to unlock, enhancing protection against unauthorized access in case of inactivity.

Q10. Do you provide end users a tool to save all passwords (preferably cloud-based for home and work use)?

A10: No, JS Bank does not provide a specific tool for end users to save passwords, aiming to avoid potential security risks associated with centralized storage of sensitive information.

Q11: Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?

A11: Yes, JS Bank has implemented a robust password policy for both administrators and users, discouraging the use of common or easily guessable passwords to enhance security measures.

Q12: Are all end point logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?

A12: Yes, JS Bank employs a sophisticated system that ingests end point logs using smart technology, integrating threat intelligence and AI to analyze threat actor activities and heuristics for proactive cybersecurity.

Q13: Do you harden all endpoints and remove everything that is not needed for job functionality?

A13: Yes, JS Bank follows a security practice of hardening all endpoints by eliminating unnecessary components, focusing on job functionality to minimize potential vulnerabilities.

Q14: Do you have next-generation anti-malware protection (e.g., managed detection and response [MDR], extended detection and response [XDR], endpoint detection and response [EDR])4 on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?

A14: Yes, JS Bank has implemented next-generation anti-malware protection across all endpoints, incorporating technologies like MDR, XDR, and EDR. This system utilizes a threat intelligence-based security analytics platform with built-in security context for enhanced protection.

Q15: Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your network?

A15: Yes, JS Bank enforces measures to prevent non-enterprise-controlled and unsecured devices from accessing any part of the network, ensuring a controlled and secure environment.

Q16: Do all endpoints have personal firewalls for accessing the Internet when not attached to the enterprise network?

A16: Yes, each endpoint at JS Bank is equipped with personal firewalls for secure Internet access when disconnected from the enterprise network, adding an additional layer of protection.

Q17: Do all endpoints have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?

A17: Yes, JS Bank ensures that all endpoints have antivirus software installed, which cannot be disabled by end users. The software is configured to receive automatic updates whenever new updates are available, maintaining the latest threat protection.

Q18: Do all endpoints have a next-generation anti-malware application installed?

A18: Yes, JS Bank has deployed next-generation anti-malware applications on all endpoints, enhancing the overall security posture with advanced malware protection measures.

Q19: Are all logs stored for at least 2 years?

A19: Yes, JS Bank ensures that all logs are stored for a minimum of 2 years, meeting regulatory requirements and providing an extensive historical record for analysis.

Q20: Are all devices generating logs?

A20: Yes, all devices within JS Bank's network generate logs, ensuring comprehensive coverage for monitoring and analysis of activities across the entire infrastructure.

Q21: Are all logs being reviewed daily by inside and/or outside sources?

A21: Yes, JS Bank conducts daily reviews of logs by both internal and external sources, enhancing the detection of any suspicious activities and ensuring a proactive response to potential security incidents.

Q22: Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?

A22: Yes, JS Bank has established a mature and well-organized cybersecurity incident response system. It includes both in-house capabilities and collaboration with third parties to ensure thorough investigations of all incidents, enhancing the overall resilience of the security infrastructure.

Q23: Do you only give employees the tools and access needed to perform their job functions, and nothing else?

A23: Yes, JS Bank strictly adheres to the principle of least privilege, providing employees with only the tools and access required for their job functions. This approach minimizes the attack surface and reduces the risk of unauthorized access or activities.

Q24: Do you utilize the principle of least privilege?

A24: Yes, JS Bank utilizes the principle of least privilege. This means that access rights and permissions are assigned at the minimum levels necessary for employees to perform their job functions, reducing the risk of unauthorized access and potential security breaches.

Q25: Do you deploy a zero-trust model?

A25: Yes, JS Bank deploys a zero-trust model. This approach ensures that trust is never assumed and that every user and device, both inside and outside the network, is continuously verified before granting access. This enhances overall security by minimizing the risk of unauthorized access and potential security threats.

Q26: Do you require multifactor authentication (MFA) for all connections outside network?

A26: Yes, JS Bank requires multifactor authentication (MFA) for all connections outside the network. This additional layer of security helps verify the identity of users accessing the network from external sources, reducing the risk of unauthorized access, and enhancing overall cybersecurity.

Q27: Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?

A27: Yes, JS Bank requires multifactor authentication (MFA) for internal authenticated network users to access key infrastructure and sensitive data inside the network, including the crown jewels. This ensures an extra layer of protection against unauthorized access and enhances the security of critical assets within the organization.

Q28: Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)

A28: Yes, JS Bank manages all credentials in an organized manner that enables the quick conduct of a password reset for every account on the network, including service accounts. This proactive approach ensures efficient credential management and enhances the overall security of the network by promptly addressing any potential security threats related to passwords.

Q29: Have you recently assessed your Active Directory to ensure that it is properly configured and secured?

A29: Yes, JS Bank recently assessed its Active Directory to ensure proper configuration and security. Regular assessments help identify and address any vulnerabilities or misconfigurations, enhancing the overall security posture of the network and ensuring the robustness of the Active Directory environment.

Q30: Are you actively monitoring the security of your Active Directory?

A30: Yes, JS Bank is actively monitoring the security of its Active Directory. Continuous monitoring is crucial for promptly detecting and responding to any security incidents or anomalies, contributing to the overall cybersecurity resilience of the organization.

Q31: Do your perimeter firewalls have a deny-all rule unless otherwise authorized?

A31: Yes, JS Bank has implemented a deny-all rule on its perimeter firewalls unless otherwise authorized. This practice enhances network security by restricting unauthorized access and potential threats at the network perimeter.

Q32: Is your demilitarized zone (DMZ) secured?

A32: Yes, JS Bank has implemented security measures to ensure the demilitarized zone (DMZ) is secured. This enhances the protection of the network by establishing a secure intermediary zone that adds an extra layer of defense against potential threats.

Q33: Has it been ensured that there are no data, databases or stored accounts on the DMZ?

A33: Yes, JS Bank ensures that there are no data, databases, or stored accounts on the DMZ. This practice enhances security by minimizing potential points of vulnerability in the demilitarized zone.

Q34: Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?

A34: Yes, JS Bank deploys anti-spoofing technology to prevent forged IP addresses from entering the network. This measure enhances the network's security by mitigating the risk of unauthorized access through IP address manipulation.

Q35: Do you prevent the disclosure of internal IP address and routing information on the Internet?

A35: Yes, JS Bank implements measures to prevent the disclosure of internal IP addresses and routing information on the Internet. This practice helps enhance security by minimizing the exposure of sensitive network details to potential attackers.

Q36: Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting Wi-Fi, confidential data, virtual machines and printers away from crown jewels)?

A36: Yes, JS Bank employs network segmentation with restrictive firewalls to separate key infrastructure from other parts of the network. This segmentation enhances security by isolating critical components such as Wi-Fi, confidential data, virtual machines, and printers, reducing the risk of unauthorized access to crown jewels.

Q37: Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?

A37: Yes, JS Bank has well-defined procedures and implementations to protect cryptographic keys used to safeguard stored data. These measures are in place to prevent the unauthorized disclosure and misuse of cryptographic keys, ensuring the security of stored data.

Q38: Are cryptographic keys stored in the fewest possible locations with at least dual custodians?

A38: Yes, cryptographic keys at JS Bank are stored in the fewest possible locations, and the bank follows a dual custodian approach to enhance the security of these keys. This ensures a robust and secure management of cryptographic keys.

Q39: Do you utilize full disk encryption on all appropriate drives?

A39: Yes, JS Bank utilizes full disk encryption on all appropriate drives. This security measure helps protect sensitive data in case of unauthorized access to physical devices.

Q40: Do you use secure encryption in motion-at least Transport Layer Security (TLS) 1.1 or higher?

A40: Yes, JS Bank uses secure encryption in motion, specifically Transport Layer Security (TLS) 1.1 or higher. This ensures the secure transmission of data over networks, safeguarding customer information during online transactions and communications.

Q41: Is all non-console administrative access encrypted using strong cryptography?

A41: Yes, all non-console administrative access at JS Bank is encrypted using strong cryptography. This security measure ensures that unauthorized access attempts are thwarted, protecting sensitive administrative information.

Q42: Do you perform periodic targeted threat hunts?

A42: Yes, JS Bank conducts periodic targeted threat hunts to proactively identify and mitigate potential threats. This approach enhances the bank's cybersecurity posture by staying vigilant against evolving security risks.

Q43: Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?

A43: Yes, JS Bank regularly ingests current threat intelligence from multiple sources and has established procedures to implement rapid countermeasures based on this information. This proactive approach helps enhance the bank's ability to respond effectively to emerging threats.

Q44: Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?

A44: Yes, JS Bank includes routine dark web reconnaissance as part of its cybersecurity strategy to gain insights into what information exists on the dark web related to its brand and enterprise structures. This practice helps the bank stay informed about potential threats and vulnerabilities.

Q45: Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?

A45: Yes, JS Bank closely monitors all vendor and third-party supply-chain connections for compliance and untoward issues as part of its cybersecurity and risk management practices. This ensures that the bank's partners adhere to security standards and do not pose potential risks to the organization.

Q46: Do you conduct at least 1 penetration test annually, performed by a third party?

A46: Yes, JS Bank conducts at least one penetration test annually, which is performed by a third party. This practice helps identify vulnerabilities and assess the effectiveness of the bank's security measures against potential cyber threats.

Q47: Do you conduct routine vulnerability scans and remediate all vulnerabilities a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?

A47: Yes, JS Bank conducts routine vulnerability scans and follows a remediation process. Vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more are addressed within 30 days, and all other vulnerabilities are remediated within 90 days. This approach ensures a timely response to identified security weaknesses, contributing to the overall cybersecurity of the bank.

Q48: Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?

A48: Yes, JS Bank routinely conducts scans on its Internet-facing infrastructure to identify and address potential penetration and vulnerabilities. This proactive measure contributes to the ongoing security assessment of the bank's external-facing systems.

Q49: Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?

A49: Yes, JS Bank performs an annual business impact analysis and risk analysis report in collaboration with both insider and outside auditors. This comprehensive assessment helps identify potential risks and impacts on the business, contributing to strategic decision-making and ongoing improvements in risk management.

Q50: Do you have an enterprise security policy that is at least updated annually and understood by all the parties to which it applies?

A50: Yes, JS Bank has an enterprise security policy that is updated annually, and efforts are made to ensure that all relevant parties, including employees and stakeholders, understand and comply with the policy. This regular updating and communication enhance the effectiveness of security measures across the organization.

Q51: Do you have a formal change control policy?

A51: Yes, JS Bank has implemented a formal change control policy. This policy outlines structured procedures for initiating, reviewing, approving, and implementing changes within the organization's IT infrastructure. The formal change control policy helps maintain the stability and security of the bank's systems.

Q52: Are processes and mechanisms for restricting physical access to servers, consoles, backup, and network equipment in place and properly safeguarded?

A52: **Yes**, JS Bank has established processes and mechanisms to restrict physical access to servers, consoles, backup, and network equipment. These measures are in place to ensure the physical security and safeguarding of critical infrastructure components.

Q53: Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?

A53: Yes, JS Bank has implemented both physical and logical controls to restrict the use of publicly accessible network jacks within its facilities. These controls contribute to the overall security of the network infrastructure and help prevent unauthorized access.

Q54: Do you have a robust cyber incident response plan (CIRP) that is reviewed and practiced yearly? The CIRP should be routinely updated, and the core and extended incident response teams should practice responses at least annually using tabletop or functional cybersecurity exercises.

A54: Yes, JS Bank has a comprehensive cyber incident response plan (CIRP) that undergoes regular reviews and annual practice sessions. Both core and extended incident response teams participate in tabletop or functional cybersecurity exercises to ensure preparedness and effectiveness in responding to potential cyber incidents

Q55: Do you have playbooks with technical instructions for handling common cybersecurity incidents?

A55: Yes, JS Bank has developed playbooks containing technical instructions for handling common cybersecurity incidents. These playbooks serve as valuable resources for incident response teams, providing structured guidance to effectively address and mitigate specific types of cyber threats.

Q56: Do you have thorough diagrams of the entire network, including Wi-Fi?

A56: Yes, JS Bank maintains thorough diagrams of the entire network, encompassing both wired and Wi-Fi components. These diagrams provide a visual representation of the network architecture, aiding in understanding and managing the overall infrastructure effectively.

Q57: Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners, and restoration? Does this inventory include instructions with time periods to recover?

A57: Yes, JS Bank maintains a comprehensive inventory of all assets, including business criticality levels, owners, co-owners, and restoration instructions. This inventory provides essential information for effective asset management and includes instructions with defined time periods for recovery in case of disruptions.

Q58: Do you have a full set of data flow diagrams?

A58: Yes, JS Bank has a complete set of data flow diagrams that illustrate the flow of information within the organization's systems. These diagrams help visualize the movement of data, enhancing the understanding of data processes and aiding in the implementation of effective security measures.

Q59: Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?

A59: Yes, JS Bank utilizes file integrity monitoring (FIM) specifically for the crown jewels of the organization. This proactive measure helps detect and respond to any unauthorized changes or alterations to critical files, ensuring the integrity and security of essential assets.

Q60: Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?

A60: Yes, JS Bank follows a data minimization approach, keeping the storage of confidential data to a minimum. Additionally, the bank ensures secure deletion of confidential data when it is no longer needed, aligning with best practices for data privacy and security.

Q61: Do you require data classification throughout the network?

A61: Yes, JS Bank implements data classification throughout its network. This ensures a structured approach to handling and protecting different types of data based on their sensitivity and importance.

Q62: Do you deploy a network and cloud-based data loss prevention (DLP) program where confidential data resides?

A62: Yes, JS Bank deploys a comprehensive data loss prevention (DLP) program both in the network and cloud environments where confidential data resides. This program helps monitor, detect, and prevent unauthorized access or leakage of sensitive information.

Q63: Do you prevent confidential data from being copied to external devices and external devices from being attached to endpoints?

A63: Yes, JS Bank implements measures to prevent the unauthorized copying of confidential data to external devices. Additionally, controls are in place to restrict external devices from being attached to endpoints, minimizing the risk of data exfiltration, and enhancing overall data security.

Q64: Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?

A64: Yes, at JS Bank, processes, and mechanisms for developing and maintaining secure systems and software are well-defined and understood. The organization follows best practices and standards in secure software development to ensure the integrity and resilience of its systems.

Q65: Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?

A65: Yes, JS Bank incorporates software engineering techniques and other methods to prevent or mitigate common software attacks and vulnerabilities in all software. This proactive approach is part of the organization's commitment to building secure and resilient software.

Q66: With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?

A66: Yes, JS Bank addresses new threats and vulnerabilities related to its public-facing web applications on an ongoing basis. Regular assessments and updates are conducted to ensure the security of these applications against evolving cyber threats.

Q67: Are these applications protected against attacks?

A67: Yes, JS Bank ensures that its public-facing web applications are protected against various cyber attacks. Security measures such as firewalls, intrusion detection systems, and regular monitoring are in place to safeguard these applications.

Q68: Are preproduction environments separated from production environments, and is separation enforced with access controls?

A68: Yes, JS Bank enforces the separation of preproduction environments from production environments, and this separation is rigorously enforced with access controls. This practice helps maintain the integrity of production systems and minimizes the risk of unauthorized access or changes during the development and testing phases.

Q69: Are all mobile devices governed by effective mobile (MDM) policies?

A69: Yes, all mobile devices at JS Bank are governed by effective Mobile Device Management (MDM) policies. These policies ensure the secure and compliant use of mobile devices within the organization.

Q70: Do you disallow any enterprise device management connectivity of mobile devices not controlled by security mechanisms?

A70: Yes, JS Bank disallows enterprise device management connectivity for mobile devices that are not controlled by security mechanisms. This policy helps maintain a secure and controlled environment, ensuring that only authorized and secure mobile devices have access to enterprise device management functionalities.

HANDWRITTEN NOTES

2014-0247
Insha Sammani
BSCS-7E

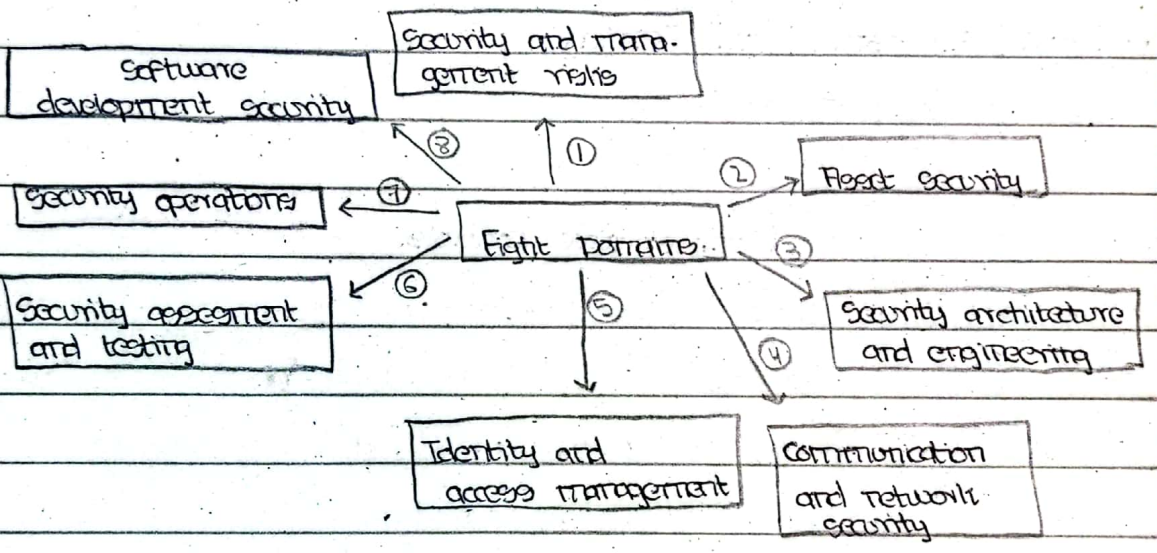
HOW TO MANAGE SECURITY RISKS AND THREATS

Date

Security Domains Overview:

CISSP ki sath 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:

- Focus: 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.

RC

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

RC

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:

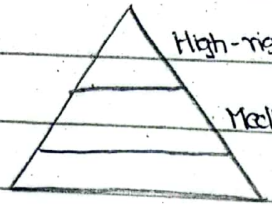
- Focus: Securing coding practices use karna throughout SDLC.

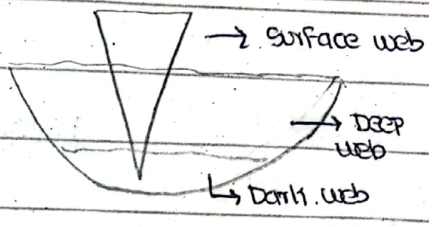
Threats, Risks, and Vulnerabilities:

- Threats: circumstances ya events jo assets ko negative way mai use karte hain. Example: Social engineering attacks, phishing.
- Risks: Confidentiality, Integrity ya Availability ko impact karne wale kuch bhi. levels (low, medium, High) mai rate kiya jai.
- Vulnerabilities: Threats exploit kiye jaa sake 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 concepts samajhne mai.

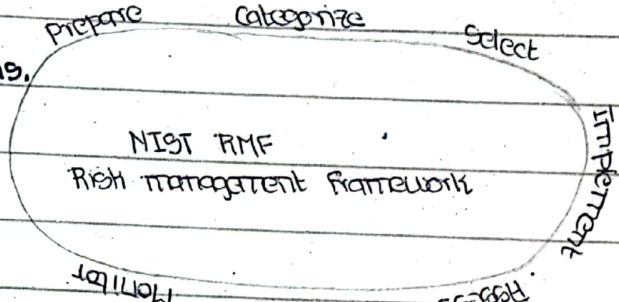
RC

Date





Impacts of Threats, Risks, and Vulnerabilities:

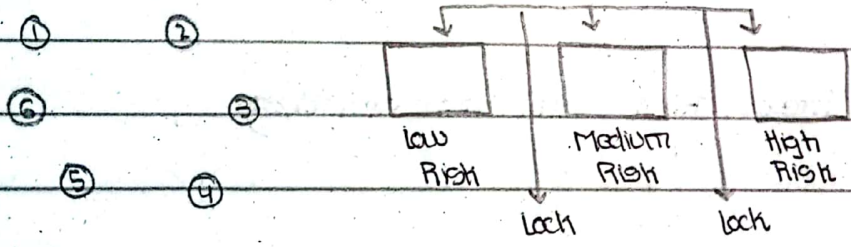


Ransomware:

- Malicious attack jo data ko encrypt karta hai aur access restore ki liye payment mangta hai.
- Organizational operations par teen 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 sath security domains, threats, risks, vulnerabilities, ransomware, aur web ki 3 layers ko cover kiya 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:

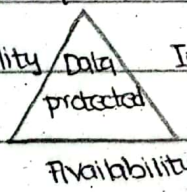
RC

Date

- Security frameworks guidelines that help risk mitigate or plans banate hi liye.
- Overlapping requirements ko organizations aur login ko protect karne hi liye use.
- Frameworks security policies aur processes banate he liye starting point provide karte hain.

Security Controls:

- Safeguards ko specific security risks ko kam karne hi liye design kiye gaye tole hain. • Common types: Encryption, Authentication, Authorization.
- CIA Triad: core security model he components - Confidentiality, Integrity, Availability.



Security Tools- Logs:

- Logs events ki record tole hain organization he 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 hai.

Security Information and Event Management (SIEM) Tools:

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

SIEM Dashboards:

RC

Date

bility]

- Dashboards information ko visual form mai present karte hain for quick understandi
- 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 hote hai
- Customizable dashboards diff organizational members ki liye relevant metrics display kar skte hain.

Types of SIEM Tools:

- Self hosted SIEM tools: Organization ki own 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.

Date

• Splunk Enterprise: Self-hosted tools for data analysis, real-time alerts, and necessary information in live.

• 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 take him to manual operations dictate have him security incidents in response mai.

• Provides structure, ensure compliance, and documentation and communication in like processes guide have him.

Incident Response Playbook:

• Six phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity, Coordination.

• Playbooks security analysts to guide have him eli consistent process mai security incidents in response mai.

Usage of Incident Response Playbook:

• Examples include malware attacks, phishing actions assessment, containment, eradication, and recovery in like define like take him.

• Playbooks living documents take him, to lessons learned and evolving threats in basis par update like gate him.

Importance of playbooks for security Analysts:

RC

Date

- Security teams frequent updates kanh train playbooks ko address kame h liye for new threats and vulnerabilities.
- Entry-level analysts ko playbooks frequent use mai help kanke train, 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.

2011-0247
Insha Samnani
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 who 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.

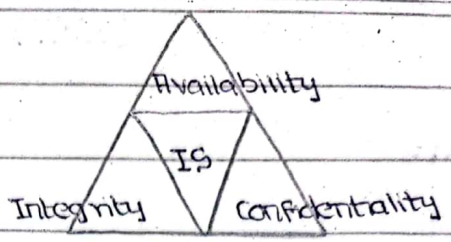
Step 1: Categorize Information System:

- 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-

RC

Date

egrity, X), (availability, X).



Information Types:

- Specific category of information (eg privacy, medical, proprietary, financial, investigation, contractor-sensitive, security management), defined by an organization 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 of risk by an authorized entity.

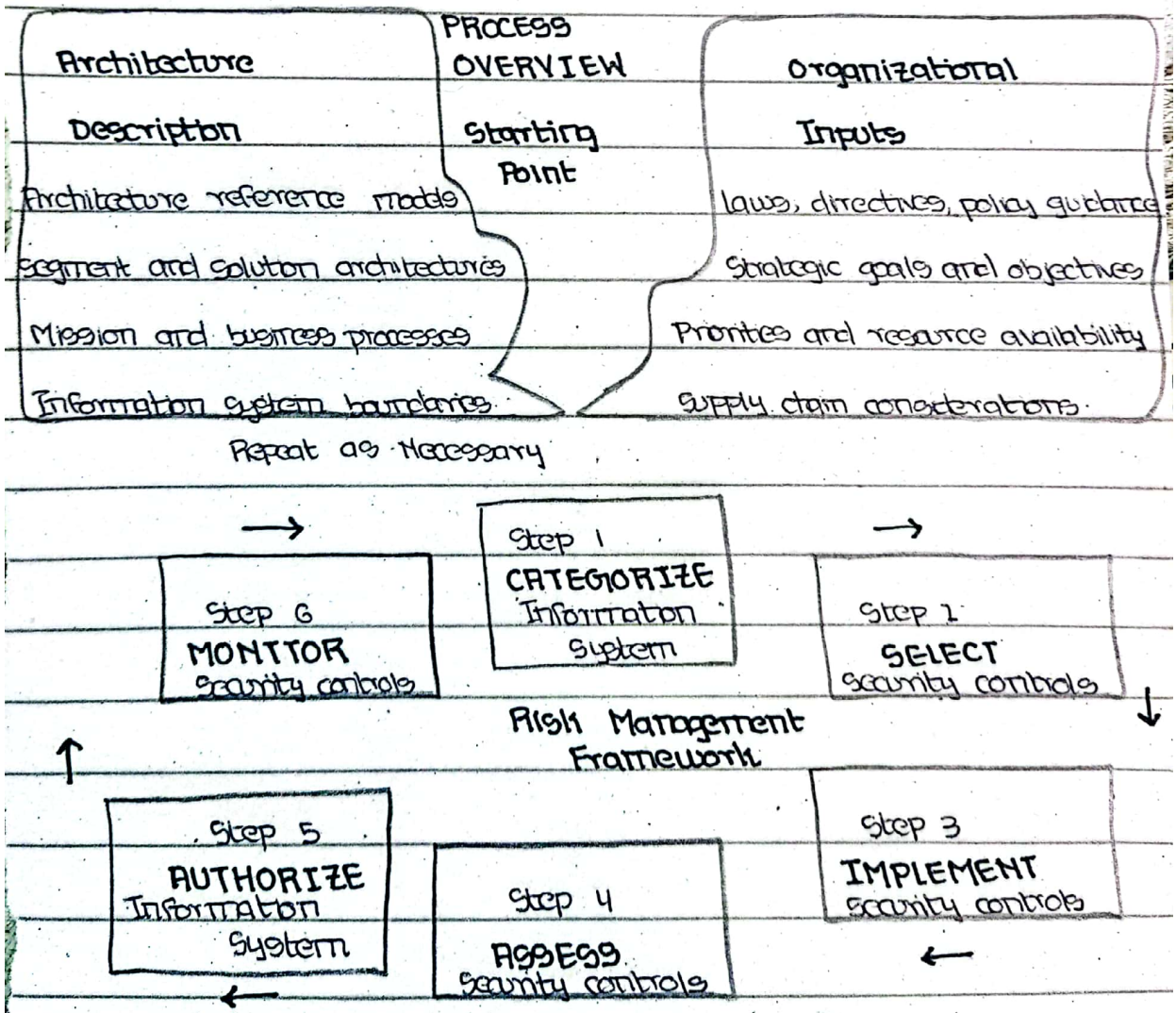
Date

Step 6: Monitor Controls:

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

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:

RC

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.

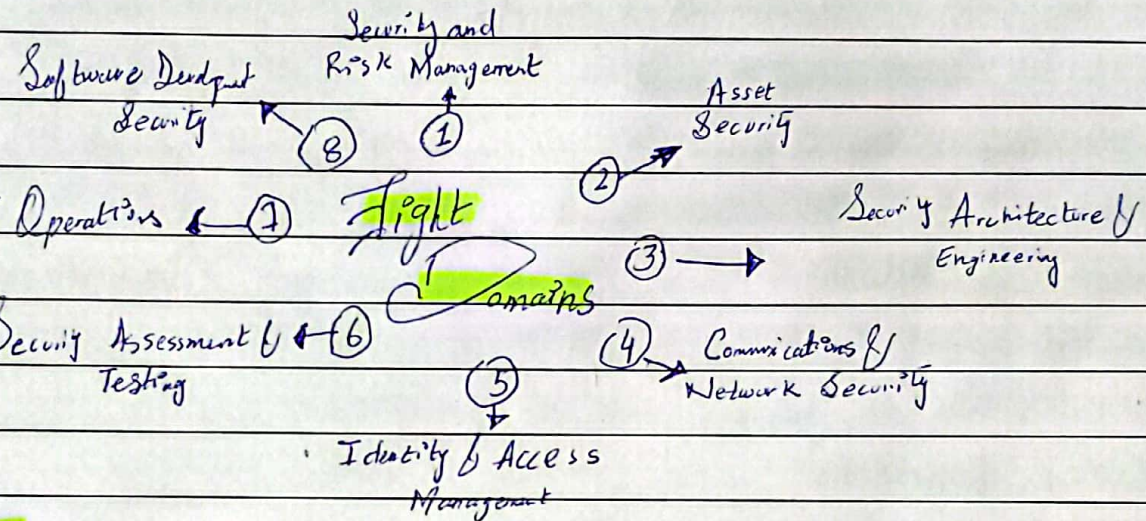
HOW TO MANAGE SECURITY RISKS & THREATS

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.

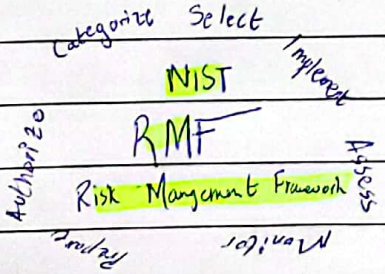
Control Name	Control Type and Explanation	Needs to be Implemented (X)	Priority
Administrative Controls			
Password Policies	Preventative, establish password strength rules to improve security / reduce likelihood of account compromise through brute force or dictionary attacks	X	High
Technical Controls			
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

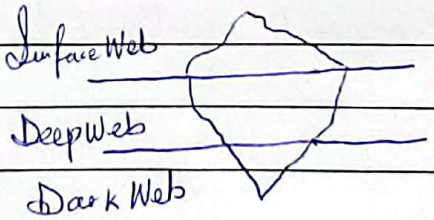
7. Security Operations :- With a focus investigations, implementing preventive measures, and conducting forensic investigations.

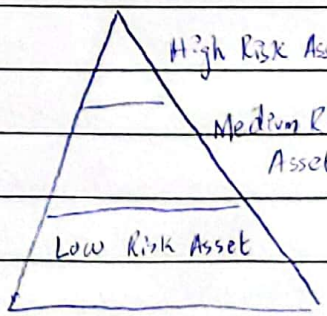
8. Software Development Security - Highlighting the use of secure coding practices throughout the software development life cycle

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 promoting security awareness







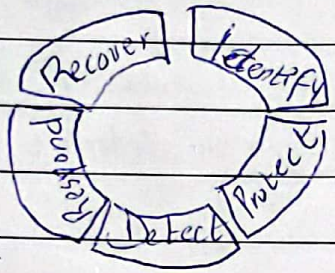
Impacts of Threats, Risks & Vulnerabilities :-

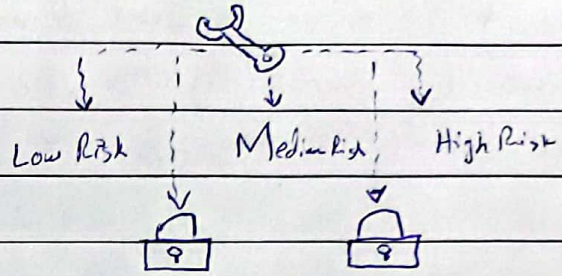
Exploring the malicious impacts of ransomware on organizational operations, including financial consequences, identity theft and reputation damage.

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:

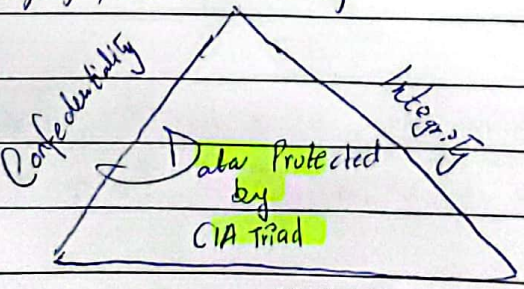
Summing the coverage of CISSP's eight security domains, threats, risks, vulnerabilities, ransomware, and the layers of the web. Highlighting the significance of the NIST RMF's 7 steps & the crucial role of entry-level analysts in maintaining security.

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

Date

Security Tools - Elkaya.

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).

Al Habib

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.

- 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.

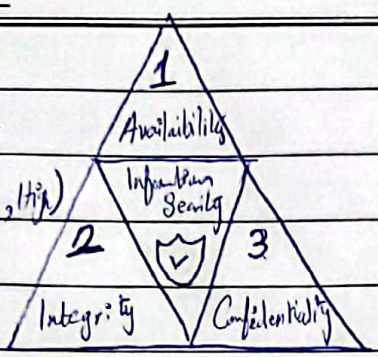
Step1: (Categorize Information System)

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.

Date _____

Example:

Security Category (SC) = (Confidentiality, High), (Integrity, High) (availability, Low)



Information Types

- Specific category of information (eg privacy, medical, proprietary, financial, investigative, 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 800-53a 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)

Continuous 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

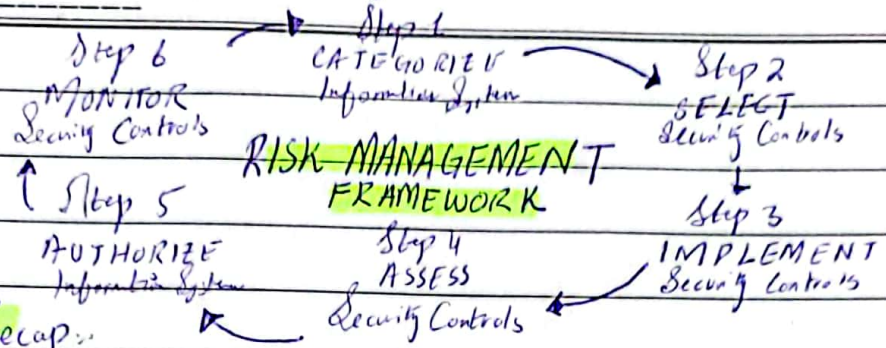
Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes Information
System Boundaries.

KRDCESS OVERVIEW
Starting Point

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

Date _____

Report on necessary



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 delving 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.

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)

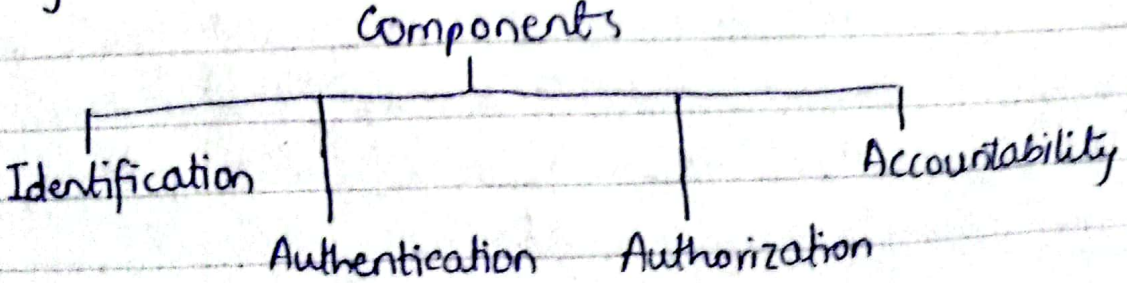
1- Security and risk management :- It deals with security goals, risk mitigation, compliance, business continuity and legal regulations. Examples include PII protection, risk procedures, compliance for internal security policies

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.

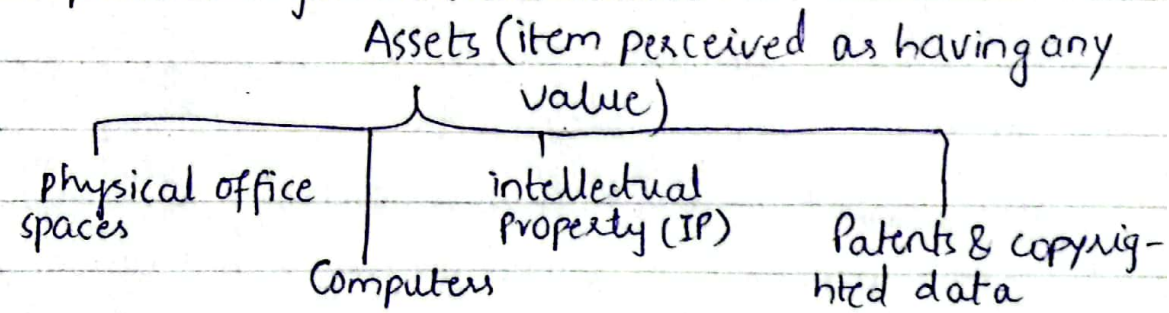


6- Security Assessment and Testing:- It focuses on security control testing, data analysis and audits. Examples include multi-factor authentication implementation.

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.



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.

*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 browsers.

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

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 kartay. 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 ju 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

minimize ongoing risks.

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

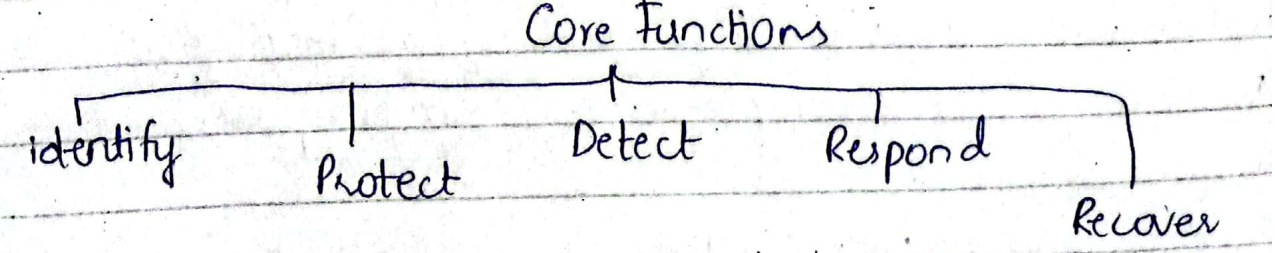
6- Authorize:- Being accountable for security and privacy risks. It involves generating reports.

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 → Bonks verifying account activity for authenticity.	- Example → banks ensure account inf is accesible Onlin

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



*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 securit 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.

-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:-

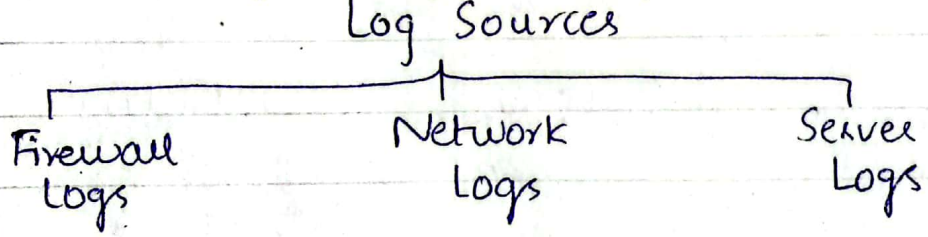
1- Controls Assessment:- Involves classifying controls into 3 categories:-

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

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.

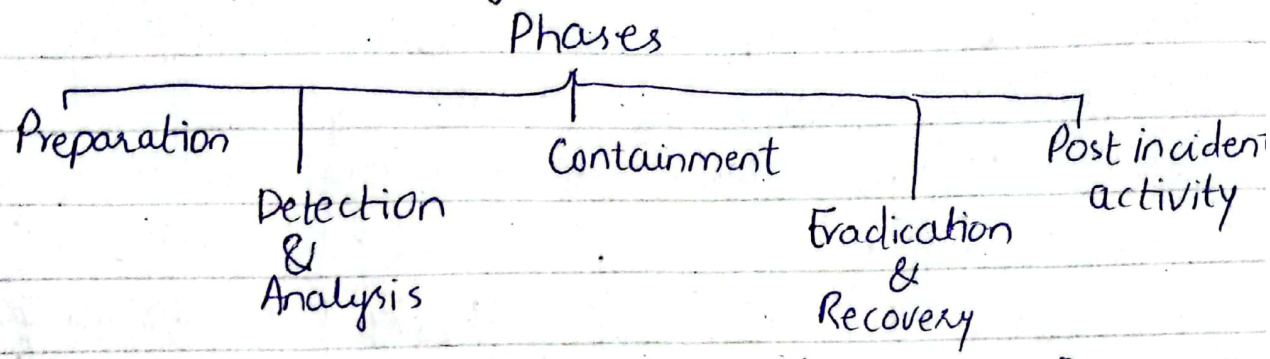


SIEM Dashboards:- Uses visual representation to provide quick insights to organization's security postures.
Display metrices such as response time and availability.

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

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

Incident Response Playbook → 6 phases



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.

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.

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.

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.