Information Security Project

Hand Written Notes of Pdf,

2 videos.

Group Members-

1) 19K-0214 — Ahmed

2) 20K-0297 — Usaid

3) 20K-0409 — Mukand

Used by Dept of Defense & US Govt
Defined in NIST 800-37 r2 (version 2)

RMF Steps

#1 Categorize Information System

Input: Architecture Description

- Architecture Reference Model
- Segment and Solution Model
- System Boundaries
- Mission & Robustness Processes

Organizational Inputs

- Laws
- Directives
- Policies
- Governance
- Strategic Goals
- Priority & Availability
- Supply Chain

eg HIPAA

Similar to Business Impact Analysis

#2 Select Security Controls

eg max tolerable downtime
Recovery Point Objective

BUT
CIA Trial in this case:

- Confidentiality
- Integrity
- Availability

Impact Values: Low, Moderate, High

Security Category = (c, value)(I, value)(A, value)
info type/info sys

eg SC_{PHI} = (C, high)(I, high)(A, low)

'protected health info' domain — not important to provide access all the time

#2 Select Security Control

Select initial set of baseline security controls for system based on security categorization, tailor and supplement security control baseline as needed based on organization assessment of risk and local conditions

eg Drone has baseline security controls that needed to be incremented when it flies into enemy country

#3 Implement and Document Security Controls

Implement then document how they are deployed within system and operation environment

#4 Assess Security Controls

Assess using appropriate procedures to determine extent to which

- controls are implemented correctly
- operating as intended
- producing desired outcome

eg reducing risk typically

NIST 800-53A gives guidance how to do it

#5 Authorize Info Sys

Authorize operations based on

Risk to: organizational ops and assets

- people
- other organizations
- Nation

Decide if that risk is acceptable formally

#6 Monitor Security Controls

Monitor and assess ongoing basis

- Assessing control effectiveness
- Documenting changes to system or env
- Conducting Security Impact Analysis
- Reporting Security State to appropriate

#7 Preparation (Optional)

Can't fully prepare for risks but some is better than none

Roll NO:

20K-0297

20K-0409

19K-0214

Roll no: 20K-0409

Why perform a Security Risk Assessment?

- Importance: Organizations regularly address security concerns due to legal requirements protecting data and public safety expectations. The goal is to identify and measure risks to information assets.

- Rational for Risk assessment

1) Cost Justification:- Extra security costs more money, but it's essential. Assessment educates manager or critical tech, risks, justifying security expenses. For example, Investing in cyber security prevents costly data breaches, saving money in the long run.

2) Productivity Improvement: Assessment enhance IT productivity, formalizing reviews, structuring information, and implementing self analysis, make everything run smoother. For example, Better security measures reduce interruptions from cyber threats, makes business operations efficient.

3) Breaking Barriers: Security decisions involve both organizational management and IT staff. Leaders decide security levels, and IT staff implements specific requirements. For example, Leaders decide on data security levels, and IT ensures transactions are secure.

4) Self Analysis: Assessment system should be simple for every one, even without security or IT expertise. This encourages ownership of security and integrates it into the organization's culture. For example, employees can follow security guidelines without advanced IT knowledge, making security a part of organization's / company's culture.

5.) Communication Boost: Assessments gather information from different parts of the organization, improving communication and decision making. For example, Sharing knowledge and potential security risks helps the whole company stay informed and respond quickly to threats.

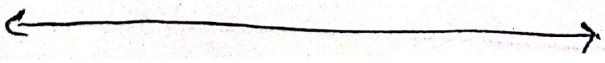
Key Procen in Info Sec.

- risk mgmt core: enterprise risk assessment and risk management processes are central to information Security.
- tailoring to org. size: Depending on the organization's size and complenity, a general prioritization might be more suitable than a detailed assessment of precise values and risks.

Frequency and Continuity

- continous activity: Security risk assessment should be ongoing.
- recommended frequency: Comprehensive Assessment should be done atleast every 2 years to explore risks. For mission-critical systems, more frequent assessments, if not continous, are highly recommended.

- Regular updates in security measure help adapt to new ~~features~~ threats and protect important information over time.



How To Manage Security Risks & Threats

Date:

What you'll learn:

Roll no: 19K-0214

- CISSP's eight security domains (Certified Information Systems security Professionals)
- Security frameworks and controls (NIST) -> (National Institute of standards & Technology)
- Security audits
- Basic Security tools
- Threats, risks and vulnerabilities
- Layers of the web

Note:

There are 8 security domains or categories identified by CISSP. Security teams use them to organize daily tasks and identified gaps in security that can cause negative consequences for an organisation and to establish their security posture.

Security Posture: An organisations ability to manage its defense of critical assets and data, and react to change.

~~The video discusses of the first four domain...~~

~~Other domains.~~

1. Security and Risk management
2. Asset security.
3. Security architecture and engineering
4. Communications and network security.
5. Identity and access management.
6. Security assesment and ~~testing~~ testing
7. Security operations.
8. Software development security.

Date: _____

Security and risk management:

Focused on defining security goals and objectives, risk ~~management~~ - mitigation, compliance, business continuity, and legal regulations.

defining security & objectives: organisations reduces risks to their critical assets and data, like PII (Personally identifiable information).

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

Compliance: Primary method used to develop an organization's internal ~~security~~ security policies, regulatory requirements, and independent standards.

Business continuity: An organizations ability to maintain their everyday productivity by establishing risk disaster recovery plans.

legal regulations: This means following rules and expectations for ethical - behaviour to minimize negligence, abuse or fraud.

Date: _____

Asset Security: Focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.

Security Architecture and Engineering: Focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data.

Note: One of the core concepts of secure design architecture is "shared responsibility"

Shared responsibility: All individuals within an organisation take an active role in lowering risk and maintaining both physical and virtual security.

Communication and network security: Focused on managing and securing physical networks and wireless communications.

- Secure Networks keep an organization's data and communications safe, whether on site, or in the cloud, or when connecting to services remotely.

For example: employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public Wi-Fi hotspots. By having security team member remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be explained by threat actors.

Date: _____

Identity and access management: Focused on access and authorization to keep data secure, by making sure users follow established policies to control and manage assets.

for example: If everyone at a company is using the same administration login, there is no way to track who has access to what data. In the event of a breach, seperating valid user activity from the threat actor would be impossible.

Components of IAM (Identity and Access Management).

- Indentification
- Authentification
- Authorization
- Accountability
- Security Assesment and Testing

Security Assesment and Testing: Focused on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.

Security Operations: Focused on conducting investigations and implementing preventative measures.

Software development security: Focused on using secure coding practices

Date: _____

→ As an entry level security analyst, one of your many roles will be to handle an organization's digital and physical ~~environment~~ assets.

Types of assets:
• Physical office • computers • customers' PII • Intellectual properties; such as, patents or copyrighted data and so much more.

∴ Unfortunately organizations ~~are~~ operate in an environment that presents multiple security threats, risks & vulnerabilities to their assets.

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

e.g: Social Engineering Attack: A manipulation technique that exploits human error to gain private information, access or valuables.

Risk: Anything that can impact the ~~confidentiality~~ confidentiality, integrity, or availability of an asset.

- Low Risk asset: Information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised.

- Medium Risk asset: Information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations.

- High Risk asset: Information protected by regulations or laws, which if compromised would have a severe negative impact on an organization's finances, ongoing operations, or reputation. This could include leaked assets with SPII, PII, or intellectual property.

Date:

Vulnerabilities: A weakness that can be exploited by a threat

* Important point: both, a vulnerability and threat must be present for there to be a risk.

Examples:
- Outdated firewall.
- Software or Applications
- weak passwords
- Un-protected confidential data.

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

Layers of the web:
- Surface web
- Deep web
- Dark web

~~Surface layer.~~

Surface web: It is the layer that most people use. It contains content that can be accessed using a web browser.

Deep web: It generally requires authorisation to access it. An organisation's internet is an example of deep web, since it can only be accessed by employees or others who have been granted access.

Dark web: It can only be accessed by using special software. The dark web generally carries a negative ~~connection~~ connotation. Since it is the prefered web layer for criminals because of the secrecy that it provides.

Date:

Key impacts of Risks, Threats & Vulnerabilities

- Financial
- Identity
- Reputation

National Institute of Standards & Technology.

NIST provides many frameworks that are used by security professionals to manage risks, threats and vulnerabilities.

NIST's "Risk Management framework" or "RMF".

7 steps in "RMF"
- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

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

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

RMF step 3: Select
Choose, Customize, and capture documentation of the controls that protect an organization.

RMF step 4. Implement
Implement security and privacy plans for the organisation.

RMF step 5: Assess
Determine if established controls are implemented correctly.

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

RMF step 7. Monitor: Be aware how systems are ~~monitoring~~ operating.

Date:

What you'll Learn

- Frameworks
- Controls
- Design principales
- Security audits.

Security Frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy. Such as ~~social~~ social engineering attacks and ransomware.

Security Controls: Safeguards designed to reduce specific security risks.

- Three ~~co~~ common types of controls:

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

Authentication: Process of verifying who someone or something is.

- more advance methods of authentication, such as Multi-Factor Authenticat, or 'MFA', challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometric, such as a fingerprint, voice, or face-scan.

Biometrics,

Unique physical characterstics that can be used to verify a person's ~~entity~~. identity.

e.g: finger-print, an eye scan, ~~and~~ or palm scan.

Date: _____

An example of social engineering attack that can exploit biometrics is "vishing"

Vishing: The ~~exploitation~~ exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.

e.g. It can be used to impersonate a person's voice to steal their identity. and then commit a crime.

Another important security control...

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

~~CIA triad~~

CIA triad: A model that helps inform how organizations consider risks when setting up systems and security policies.

Confidentiality: Only authorized users can access specific assets or data.

Integrity: The data is correct, authentic, and reliable

Availability: Data is accessible to those who are authorized to ~~[redacted]~~ access it.

NIST Frameworks:

NIST Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best ~~practices~~ practices to manage cybersecurity risk.

- It consists of 5 important core functions,
  - Identify, Protect, Detect, Respond, Recover

NIST S.P. 800 - 53

A unified framework for protecting the security of information systems within the federal government.

Identify: The management of cybersecurity risk and its effect on an organizations people and assets.

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

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

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

Recover: The process of returning affected systems back to normal-operation.

Date:

OWASP (Open Web Application security projects). principles

- Minimise the attack surface area:
- Principle of least privilege
- Defense in depth
- Seperation of duties
- Keep security simple
- Fix Security issues correctly.

- how they all work together?
- by conducting Security audits.

Security audit: A review of an organisation's security controls, policies, and, procedures against a set of expectations.

Purposes of internal security audits:

- Identify organizational risk
- Assess controls
- Correct compliance issues

Common elements of internal audits:

- Establishing the scope and goals
- Conducting a risk assessment
- Completing a controls assesment.
- Assessing compliance
- Communicating results.

Date:

1. Establishing scope and goals:
   - Scope refers to the specific criteria of an internal security audit.
   - Goals are an outline of the organization's security objectives.

Scope: The internal IT audit will assess the following:
- Assess user permissions
- Identify existing controls, policies and procedures
- Account for technology currently in use

Goals: The goals for the internal IT audit are:
- Adhere to the NIST Cybersecurity Framework (CSF)
- Establish policies and procedures to ensure compliance with regulations.
- Fortify system controls

2. Conducting a risk assessment.

Risk description: There is a lack of proper management of physical and digital assets; equipment used to store data is not properly secured; and access to private information in the organization's internal network needs more robust controls in place.

Control categories

- Administrative controls
- Technical controls
- Physical controls

Date: _____

Administrative Controls			
Control name	Control type and explanation	Needs to be implemented (X)	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			
Control name	Control type and explanation	Needs to be implemented (X)	Priority
Intrusion-Detection system (IDS)	Detective; allows IT team to identify possible ~~functions~~ intrusions (i.e: anomalous traffic) quickly.	X	High
Encryption.	Deterrent; makes confidential information/data more secure (i.e, website payment transactions)	X	High

Date: _____

Physical controls			
Control-name	Control type and explaination	Needs to be implemented (X)	Priority
Closed-circuit television (CCTV) surveillance	Preventative / detective; can reduce risk of certain events; can be used after event for investigation	X	High
Locks	Preventative; physical and digital assets are more secure	X	High

Note: Compliance regulations are laws that organizations must follow to ensure private data remain secure.

The final common element of an internal security audit is ~~"communication"~~. "communication"

Once the internal security audit is complete, results and recommendations need to be communicated to stakeholders.

Stakeholder communication

- Summarizes scope and goals
- Lists existing risks.
- Notes how quickly those risks need to be addressed
- Identifies compliance regulations.
- Provides recommendations.

Date:

What you'll Learn

- Logs
- SIEM dashboards
- Common SIEM tools

Log: A record of events that occur within an organization's systems and networks.

Common log sources:

- Firewall logs
- Network logs
- Server logs

A Firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

A server log is a record of events related to services, such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

SIEM dashboard:

SIEM solutions rely on dashboards to collect and analyze log data from various sources, providing actionable insights for analysis and normalization.

Date: _____

Security Information and event management (SIEM)

An application that collects and analyzes log data to monitor critical activities in an organization.

Different types of SIEM tools

- Self-hosted
- Cloud-hosted
- Hybrid

Note: Splunk Enterprise, Splunk cloud, and chronicle are common SIEM tools that many organisations use to help protect their data and systems.

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

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

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

Date:

What you'll learn

- Playbooks
- Six phases of incident response

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

It also clarify what tools should be used in response to a security incident.

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

Incident response playbook phases:

- Preparation
- Detection and analysis.
- Containment
- Eradication and recovery
- Post incident activity
- Coordination

Preparation: Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users.

Detection and analysis: This phase detect and analyze events using defined processes and technology.

Date: _____

Containment: Its goal is to prevent further damage and reduce the immediate impact of a security incident.

Eradication and recovery: It involves the complete removal of an ~~incident~~ incidence artifacts, so that an organization can return to normal operations.

Post incident activity: It includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organisation is better prepared to handle future incidents.

Coordination: It involves reporting incidents and sharing information throughout the incident response process based on the organization's established standards.

Note: SIEM tools and playbooks work together to provide a structured and efficient way of responding security incidents.