Chapter 2 – Personnel Security and Risk Management Concepts

Personnel Security

- What is the weakest link and why?

Personnel Security

- To apply security governance, we must address the weakest link in this chain – people
- On the flip side, this is our greatest security asset when properly trained
- Users, developers, managers, vendors, consultants, etc.

Job Descriptions and Responsibilities

- Job Description
- Job Responsibilities
- Candidate Screening

Onboarding

- Security-focused organization, the process of onboarding will be heavily on security policies
- Identity and Access Management (IAM)
- Principle of Least Privilege
- Employment Agreement
- Acceptable Use Policy (AUP), Nondisclosure Agreement (NDA), Non-Compete (CNC)

Employee Oversight

- Mandatory Vacations
- Collusion – Several people working to commit a crime
- User Behavior Analytics (UBA) and User and Entity Behavior Analytics (UEBA)

Offboarding, Transfers, Termination

- Offboarding is the removal of an employee’s identity from the IAM system once that person left
- Transfers is when there’s a position, department, or organizational change
- A strong relationship between the security and HR department is highly needed

Offboarding, Transfers, Termination

- Termination is to reduce the risk while treating the person with respect
- Exit interview is to understand why an employee is leaving and their experience

Risk Management Concepts

- Risk management is the process of identifying factors that could damage or disclose assets, evaluate those factors in light of asset value and countermeasure cost, and implement cost effective solutions for mitigating or reducing risk.

Risk Management Concepts

- There are two primary elements:
  - Risk Assessment
  - Risk Response
- Risk Awareness

Risk Terminology and Concepts

- Asset
- Asset Valuation
- Threats
- Threat Agent/Actors
- Threat Events
- Threat Vector

Risk Terminology and Concepts

- Vulnerability
- Exposure
- Risk
- Safeguards
- Attack
- Breach

Risk Terminology and Concepts

- Hazard

Risk Terminology and Concepts

- **Assets** → which are endangered by → **Threats** → exploit → **Vulnerabilities** → which results in → **Exposure** → which is → **Risk** → which is mitigated by → **Safeguards** → which protects → **Assets**

Asset Valuation

- Asset based risk analysis
- Think about it?
- Is this easy to do?

Identify Threats and Vulnerabilities

- NIST SP 800-30r1 Appendix D (Threat Sources) and Appendix E (Threat Events)
- The Consultant Cavalry

Risk Assessment/Analysis

- Risk is all relative and there’s no way to eliminate 100% of all risk
- Quantitative Risk Analysis
- Qualitative Risk Analysis
- Both are needed in cybersecurity

Qualitative Risk Analysis

- Scenario-based, perception-based, gut reaction-based
- Judgment, intuition, and experience
- NIST SP 800-30 rev 1 (Tables D-3, D-4, D-5, D-6, and E-4) csrc.nist.gov/pubs/sp/800/30/r1/final
- Delphi Technique aka anonymous surveys

Quantitative Risk Analysis

- Probability indication or a numeric indication
- Asset valuation and threat identification
- There are six major steps but can vary from organization to organization

Quantitative Risk Analysis

- Assign asset value (AV)
- Calculate exposure factor (EF)
- Calculate single loss expectancy (SLE)
- Asses the annualized rate of occurrence (ARO)
- Derive the annualized loss of expectancy (ALE)
- Perform cost/benefits analysis of countermeasures

Exposure Factor (EF)

- The percentage of loss that an organization would experience if a specific asset were violated by a realized risk
- Also know as loss potential

Single-Loss Expectancy (SLE)

- The potential loss associated with a single realized threat against a specific asset
- SLE = AV * EF
- SLE sometimes is skipped over as ALEs are the most commonly needed value for criticality prioritization

Annulized Rate of Occurrence (ARO)

- Expected frequency with which a specific threat or risk will occur within a single year
- Very complicated to calculate and is known to be probabilistic determination

Annulized Loss Expectancy (ALE)

- The possible yearly loss of all instances of a specific realized threat against a specific asset
- ALE = SLE * ARO
- ALE = AV * EF * ARO
- This is for EACH asset, largest to smallest
- Cost vs Benefit of Security Control

Risk Responses

- Mitigation or Reduction
- Assignment or Transfer
- Deterrence
- Avoidance
- Acceptance
- Reject or Ignore

Risk Responses

- Risk Appetite: total amount of risk that an organization is willing to shoulder across all assets
- Risk Capacity: the level of risk an organization is able to shoulder
- Risk Tolerance: the level of risk that an organization will accept
- Risk Limit: the max level that can be tolerated

Risk Mitigation

- Reducing Risk
- Risk Mitigation
- Safeguards, security controls, countermeasures
- Examples: firewalls, encryptions, segmentation, etc.

Risk Assignment

- Assigning Risk
- Transferring Risk
- Cybersecurity insurance, outsourcing

Risk Deterrence

- Auditing, security cameras, warning banners, guards, etc.

Risk Avoidance

- Alternative options
- Less risky endeavors

Risk Acceptance

- Cost of security is more than the actual loss
- Management has agreed to accept it
- Needs a clearly written statement why something wasn’t implemented and who is responsible for the decision

Risk Rejection

- Reject Risk
- Ignore Risk
- Unacceptable Response
- This is considered negligence in court

Risk Responses

- Inherent Risk – Default risk in the environment
- Residual Risk – After safeguards are in place, the risk that remains
- Total Risk – Amount of risk if no safeguards were in place
- Control Gap – Amount of risk reduce from safeguards

Risk Responses

- Total Risk – Controls Gap = Residual Risk
- Security must be continually maintained and monitored

Cybersecurity Insurance

- What is this?

Cybersecurity Insurance

- Coverage for Data Breaches
- Financial Loss Protection
- Legal Liabilities
- Reputation Management
- Business Interruption
- Ransomware Protection

Cybersecurity Insurance

- Forensic Services
- Incident Response
- Regulatory Compliance
- Third-Party Liability

Countermeasure Selection

- The cost of the control should be less than the value of the asset
- The cost of the control should be less than the benefit of the countermeasure
- The result of applied countermeasures should make the cost of an attack greater for the attacker than the derived benefit from an attack

Countermeasure Selection

- The countermeasure should provide a solution to a real and identified problem
- The benefit of the countermeasure should not be dependent on its secrecy.
- The benefit of the countermeasure should be testable and verifiable

Countermeasure Selection

- The countermeasure should provide a solution to a real and identified problem
- The benefit of the countermeasure should not be dependent on its secrecy.
- The benefit of the countermeasure should be testable and verifiable

Countermeasure Selection

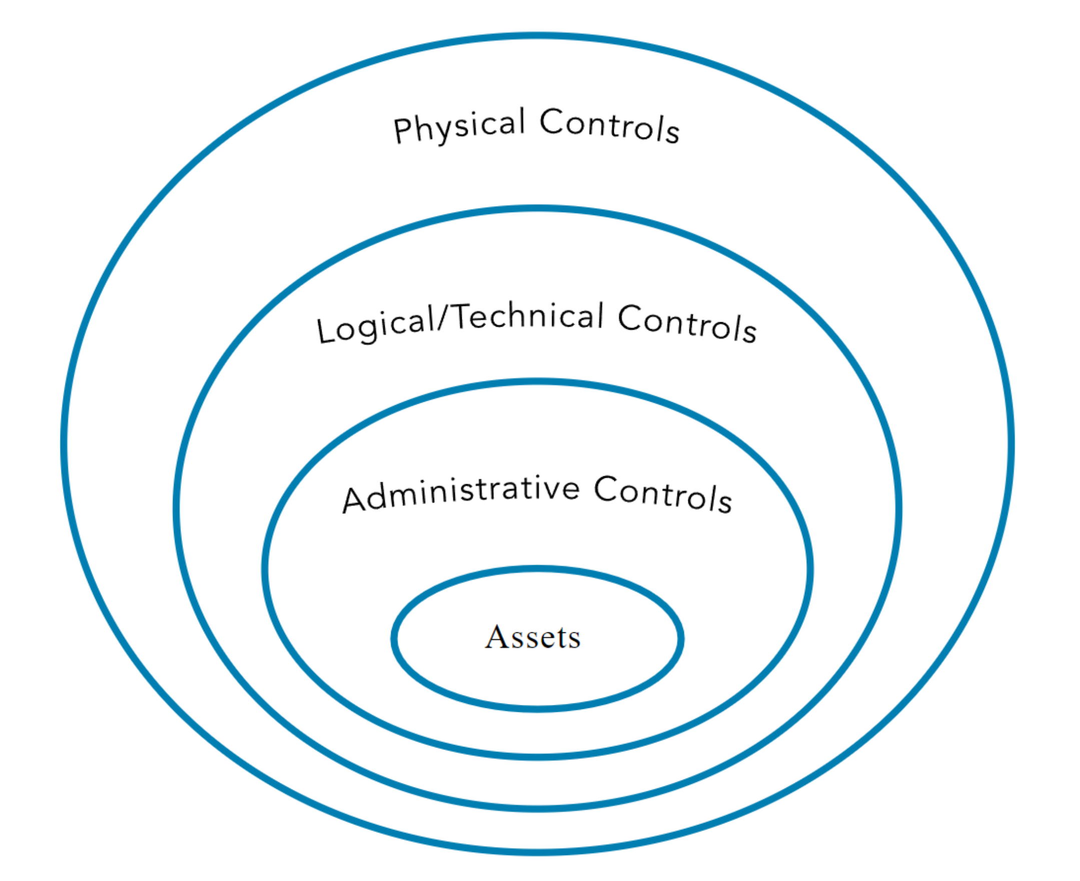
- The countermeasure should provide consistency protection across all users, systems, protocols, etc.
- The countermeasure should have few or no dependencies to reduce cascade failures
- The countermeasure should require minimal human intervention after initial deployment

Countermeasure Selection

- The countermeasure should be tamperproof
- The countermeasure should have overrides accessible to privileged operators only
- The countermeaure should provide fail-safe and fail-secure options
- KEEP IN MIND: security should be designed to support the business tasks and functions

Countermeasure Selection

- Defense in depth



Administrative Controls

- Policies and procedures defined by security policy and other regulation or requirements
- Management Controls, Managerial Controls, Procedural Controls
- Examples: policies, procedures, hiring practices, background checks, data classifications, security training, etc.

Technical or Logical Controls

- The hardware/software mechanisms used to manage access and protection for IT resources and system
- Examples: passwords, smartcards, biometrics, encryption, IDS/IPS, firewalls, ACLs, etc.

Physical Controls

- Providing protection to the facility and real-world objects
- Examples: guards, fences, motion detection, locked doors, sealed windows, lights, cable protection, laptop locks, badges, guard dogs, cameras, alarms, etc.

Applicable Types of Controls

- Preventive
- Detection
- Corrective
- Recovery
- Deterrent
- Directive
- Compensating

Preventive Control

- Deployed to stop unwanted or unauthorized activity from occurring
- Examples: fences, locks, DLP, pentesting, encryption, auditing, antimalware software, firewalls, IPSs, etc.

Detection Control

- Deployed to discover or detect unwanted or unauthorized activity
- Examples: security guards, motion detectors, CCTV, job rotation, mandatory vacations, honeypots/honeynets, IDS, incident investigation, etc.

Corrective Control

- Modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred
- Examples: installing a spring on a door so that it will close and relock, file integrity checking tools like sigverif to see boot files, etc.

Recovery Control

- An extension of corrective controls but more advanced and complex
- Examples: backups, fault-tolerant drive systems, system imaging, server clustering, antimalware software, VM shadowing, hot/warm/cold sites, etc.

Deterrent Control

- Deployed to discourage security policy violations
- Examples: security awareness training, locks, fences, security badges, guards, cameras, etc.

Directive Control

- Deployed to direct, confine, or control the actions of subject to force or encourage compliance with security policies
- Examples: policy requirements, escape route exits, monitoring, supervision, etc.

Compensating Control

- Deployed to provide various options to other existing controls to aid in the enforcement and support of security policies
- Examples: if a preventive control fails, then the compensating control takes over, DRP, etc.

Security Control Assessment (SCA)

- Formal evaluation of a security infrastructure’s individual mechanisms against a baseline or expectation
- NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

Monitoring and Measurement

- If a security control's benefits cannot be quantified, evaluated, or compared, then it does not actually provide any security

Risk Reporting and Documentation

- Risk reporting is a key task to perform at the conclusion of a risk analysis
- Internal Reporting
  - Decision-making
  - Risk Mitigation
  - Management of Risk
  - Risk Register, Risk Heat Maps, Key Risk Indicators

Risk Reporting and Documentation

- External Reporting
  - Transparency
  - Risk Profile
  - Risk Exposure
  - Risk Management

Risk Reporting and Documentation

- Risk Register/Risk Log
  - Identifying risks
  - Evaluating the severity of and prioritizing those risks
  - Prescribing responses to reduce or eliminate the risks
  - Tracking the progress of risk mitigation

Continuous Improvement

- Security is always changing, so any implemented security solution requires updates and changes over time
- Enterprise Risk Management (ERM) program can be evaluated using the Risk Maturity Model (RMM)

Continuous Improvement

- Risk Maturity Model (RMM) Levels
  - Ad Hoc
  - Preliminary
  - Defined
  - Integrated
  - Optimized

Legacy Risk

- Often overlooked
- End of Life (EOL)
- End of Service Life (EOSL) or End of Support (EOS)
- Example: Windows 10 EOSL as of October 14, 2025

Risk Frameworks

- A guideline for how risk is assessed, resolved, and monitored
- Risk Management Framework (RMF)
  - Established mandatory requirements for federal agencies
- Cybersecurity Framework (CSF)
  - Critical infrastructure and commercial organizations

Cybersecurity Framework (CSF) 2.0

- Identify: Understand and catalog assets, risks, and vulnerabilities
- Protect: Implement safeguards to protect assets and data
- Detect: Develop and deploy mechanisms for identifying and detecting security incidents
- Respond: Define strategies and process for responding to and mitigating cybersecurity incidents
- Recover: Develop and implement strategies for recovery and resilience after a cybersecurity incident
- Govern: Establish, communicate, and oversee roles, responsibilities, and policies that ensure a proactive and adaptive approach to cybersecurity

Cybersecurity Framework (CSF) 2.0

- Released in early 2024
- Not a checklist but a support and improvement of security over time
- More of a improvement system rather than a risk management process

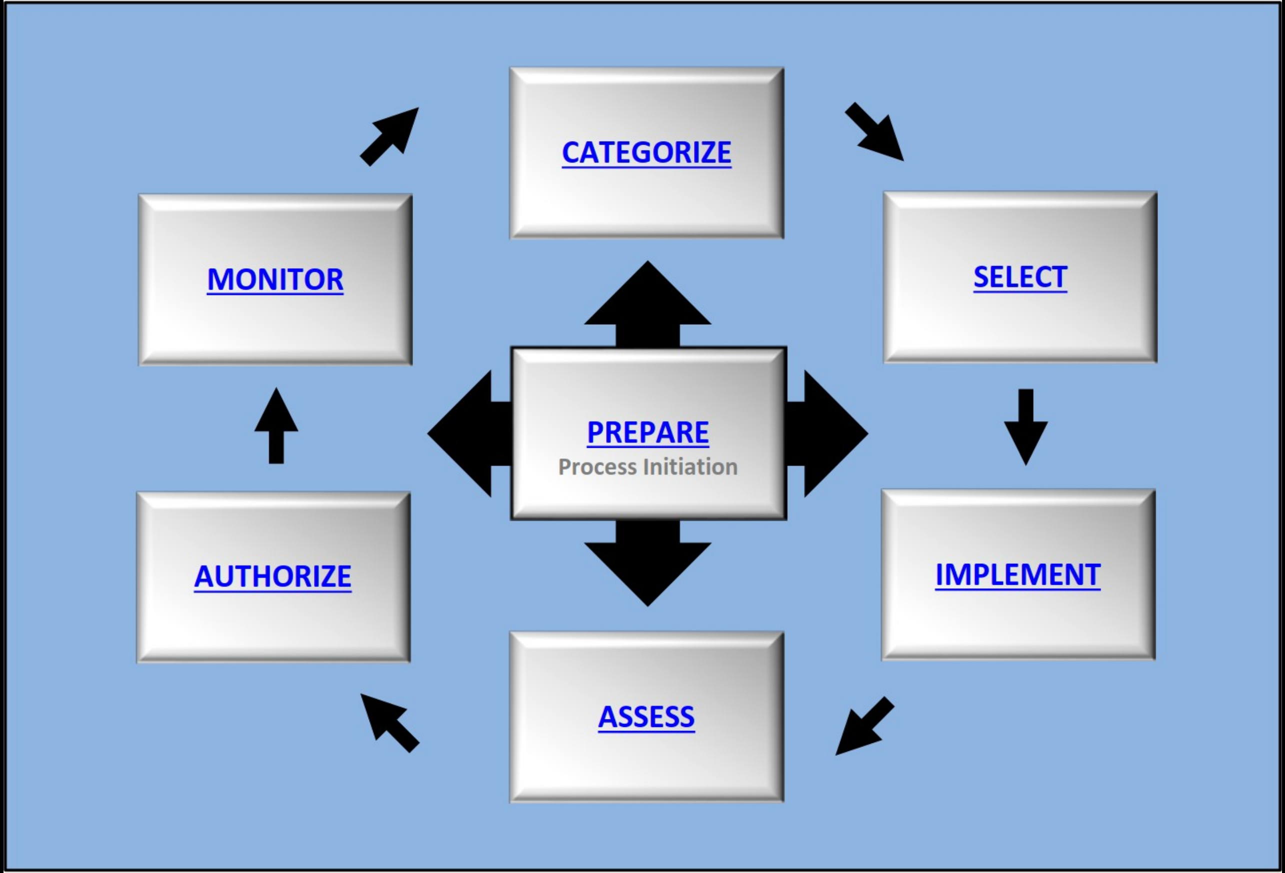
Risk Management Framework (RMF)

- NIST SP 800-37 Rev 2
- Used by US federal government
- Intended to be used as a risk management process
- There are seven phases, six which are used cyclically

Risk Management Framework (RMF)

- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

Risk Management Framework (RMF)



Other Risk Frameworks

- ISO/IEC 31000 (Risk Management – Guidelines)
- ISO/IEC 27005 (Information Security, Cybersecurity, and Privacy Protection: Guideance on Managing Information Secuirty Risks)
- www.iso.org/standard/56610.html

Other Risk Frameworks

- The Committee of Sponsoring Organizations (COSO) of Treadway Commission’s Enterprise Risk Management Integrated Framework
- ISACA’s Risk IT Framework
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

Other Risk Frameworks

- Factor Analysis of Information Risk (FAIR)
- Threat Assessment and Remediation Analysis (TARA)

Other Risk Frameworks

- The CISSP is focused in on NIST RMF
- It is important to understand other frameworks depending on what works for an organization

Social Engineering

- Exploiting human nature and behavior
- People are always the weakest link
- This works well because we’re human

Social Engineering Principles

- Authority: Effective technique because most people are likely to respond to authority with obedience
- Intimidation: Uses authority, confidence, or even the threat of harm to motivate someone to follow orders or instructions

Social Engineering Principles

- Consensus: The act of taking advantage of a person’s natural tendency to mimic what others are doing or are perceived as having done in the past
- Scarcity: Convince someone that an object has a higher value based on the object’s scarcity

Social Engineering Principles

- Familiarity: Attempts to exploit a person’s native trust in that which is familiar
- Trust: An attacker working to develop a relationship with a victim
- Urgency: The need to act quickly
- Eliciting Information: Collecting information from systems or people

Social Engineering Principles

- Prepending: Adding of a term, expression, or phrase to the beginning or header of some other communication
- Phishing: Focused on stealing credentials or identity information from any potential target
- Smishing: SMS over text messaging services

Social Engineering Principles

- Vishing: Phishing done over any telephony or voice communication systems
- Spear Phishing: Targeted version of phishing where the message is crafted and directed specifically to a group or individual
- Whaling: Spear phishing but for specific high value individuals

Social Engineering Principles

- Spam: Any type of communication that is undesired and/or unsolicited
- Shoulder Surfing: An in-peson form where someone is able to watch a user’s keyboard or their display

Social Engineering Principles

- Invoice Scams: Attempt to steal funds from an organization or individuals through the presentation of a false invoice, often followed by strong inducements to pay
- Hoax: Convince targets to perform an action that will cause problems or reduce their IT security

Social Engineering Principles

- Impersonation: Taking on the identity of someone else
- Tailgating: Unauthorized entity gains access to a facility under the authorization of a valid worker without their knowledge

Social Engineering Principles

- Dumpster Diving: Act of digging through trash, discarded equipment, or abandoned locations in order to obtain information about a target
- Identity Theft: Act of stealing someone’s identity
- Identity Fraud: Falsely claim to be someone else through the use of stolen information form the victim

Social Engineering Principles

- Typosquatting: Employed to capture and redirect traffic when a user mistypes the domain name
- Influence Campaigns: Attacks that attempt to guide, adjust, or change public opinion
- Hybrid Warfare: www.globalknowledge.com/us-en/resources/resource-li

Social Engineering Principles

- Social Media: Based on nation-state actors
- Hybrid Warfare: https://www.globalknowledge.com/us-en/resources/resource-library/white-papers/cyberwarfare-origins-motivations-and-what-you-can-do-in-response/

Security Awareness and Education

- Awareness: Bring security to the forefront
- Training: Teaching the people
- Education: Students and users learn much more than they actually need to know to perform their work tasks
- Effectiveness Evaluation