Cybrary.IT

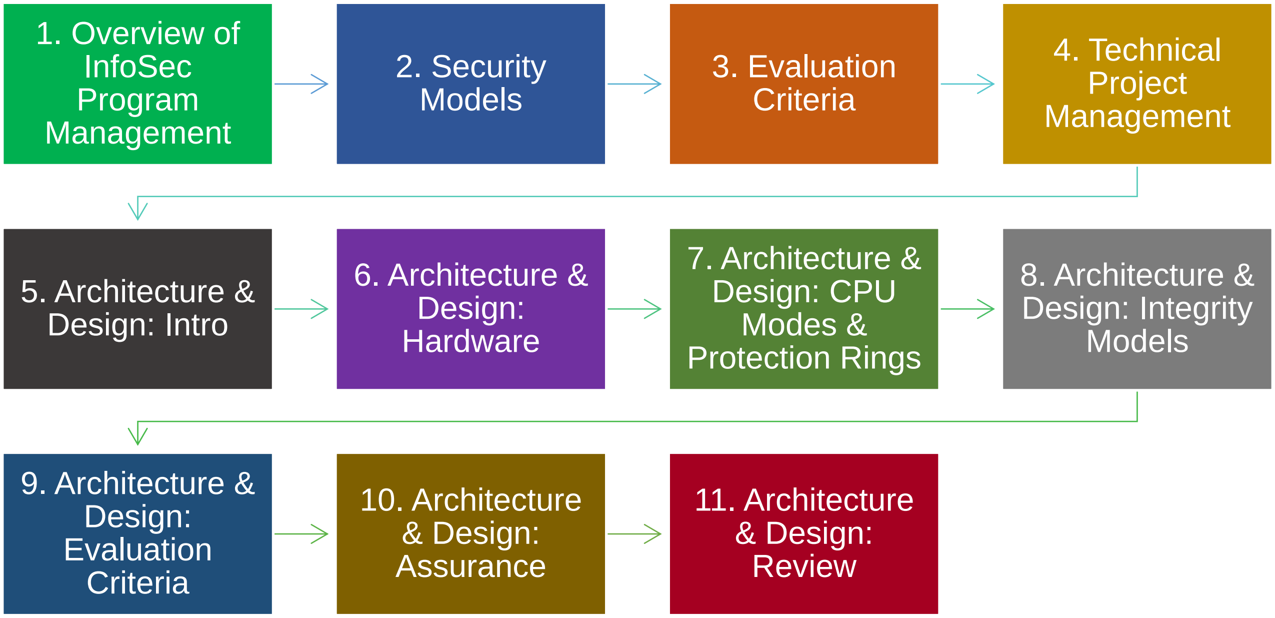
Cybersecurity Enterprise Guidelines

Ivan V. Santos

2017

Contents

I. ENTERPRISE SECURITY ARCHITECTURE:



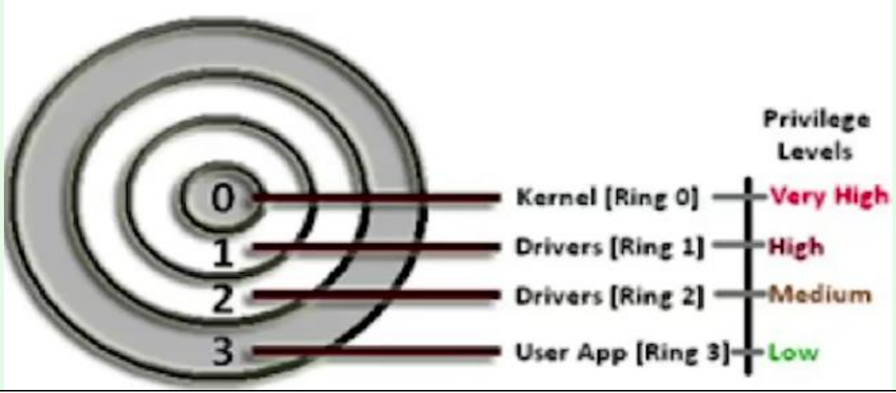
1. Overview of InfoSec Program Management → 2. Security Models → 3. Evaluation Criteria → 4. Technical Project Management → 5. Architecture & Design: Intro → 6. Architecture & Design: Hardware → 7. Architecture & Design: CPU Modes & Protection Rings → 8. Architecture & Design: Integrity Models → 9. Architecture & Design: Evaluation Criteria → 10. Architecture & Design: Assurance → 11. Architecture & Design: Review

1. Overview of InfoSec Program Management

Cost/Benefit Analysis

- Understand CBA before you do design; *the goal of security is just to support the business, you only need enough security for that – think of the $$.
- **Quantitative review**
    - AV*EF = SLE
    - SLE*ARO = ALE
    - ALE (before) – ALE (after – cost of the control = ROI
- Other costs associated with security
    - Performance
    - Ease of use
    - Backwards compatibility
    - User acceptance

Security Architecture

- **Trusted Computing**
    - Operating systems are often designed upon a ringed architecture to isolate protection layers (layers of trust):
    - 

  - Ring 0 = TCB (trusted computer base)

      - *Microsoft Word = program / application → If I open Word it is loaded into memory and becomes a process → then every individual instruction within Word is a thread

Architecture Vulnerabilities

- **Covert channels**: hidden means of communication
  - Storage: data laced somewhere unexpected
  - Timing: communication through modulation of resources
- **Maintenance hooks**: allow easy access for programmers to access code. Must be removed.
- **TOC/TOU** (time of check / time of use): a type of race condition that creates a variation between when a file is verified and when it is used. Attacks on the timing of a system.
- A system must be designed to fail in such a way that it's resources are secure
  - Secure state model
  - Fail secure
  - Maintenance secure

2. Security Models

- GOAL: build a product to be secure
- Mathematical instructions to create secure systems
- Primarily to enforce confidentiality or integrity
- Conceptual basis for system design and control implementation

Security Models

- **State machine models**
- ****The Bell-LaPadula Model**
- ****The Biba Model**
- **The Clark-Wilson model**
- **The Brewer & Nash model**
- **The information flow model**
- **The non-interference model**
- **The Lattice model**

State Machine Models (Secure State Model)

- *a system must be secure in all states of operation, or it is not secure – the basis of all security models
- The state of a system is its snapshot at any one moment. The state machine model describes subjects, objects, and sequences in a system. The focus of this model is to capture the system's state and ensure its security.
- When an object accepts input, the value of the state variable is modified. For a subject to access this object or modify the object value, the subject should have appropriate access rights.
- State transitions refer to activities that alter a systems state.

**Bell & LaPadula*

- Developed by David Elliot Bell & Len LaPadula
- This model focuses on data confidentiality and access to classified information.
- A formal model developed for the DoD multilevel security policy
- This formal model divides entities in an information system into subjects and objects

- Model is built on the concept of a state machine with different allowable states (i.e. secure state)
- **3 RULES**:
    - Simple security property – “no read up”
        - A subject cannot read data from a security level higher than subject’s security level
    - *_Security Property (pronounced Star Security Property) – “no write down”
        - A subject cannot write data to a security level lower than the subject’s security level.
    - Strong *(star) Property – “no read/write up or down”
        - A subject with read/write privilege can perform read/write functions only at the subject’s security levels.
    - TIP: simple always talks about “read”, *(star) always talks about “write”

Biba Integrity Model

- Biba is concerned with integrity
    - Developed by Kenneth J. Biba in 1977 based on a set of access control rules designed to ensure data integrity.
    - No subject can depend on an object of lesser integrity
    - Based on a hierarchical lattice of integrity levels
    - Authorized users must perform correct and safe procedures to protect data integrity
    - **RULES**:
        - Simple integrity axiom – “no read down” – a subject cannot read data from an object of lower integrity level.
        - *(star)integrity axiom – “no write up” – a subject cannot write data to an object at a higher integrity level.
        - Invocation property – a subject cannot invoke (call upon) subjects at a higher integrity level.

Clark-Wilson Model

- SIMPLE: Clark-Wilson basically says: keep users out of your stuff or they will break it
    - give the users a front-end application that has access to the database instead of direct access
- Clark Wilson enforces well-formed transactions using the access triple:
    - User → (TP) transformation procedure → CDI (constrained data item)
- Deals with all three integrity goals
- Separation of duties
    - Prevents unauthorized users from making modifications
    - Prevents authorized users from making improper modifications
    - Maintain internal and external consistency – reinforces separation of duties

Brewer-Nash Model – aka Chinese Wall

- Developed to combat conflict of interest in databases housing competitor information
- Publish in 1989 to ensure fair competition
- Defines a wall and a set of rules to ensure that no subject accesses objects on the other side of the wall
- Way of separating competitor’s data within the same integrated database

Information flow model

- Hold data in distinct compartments
- Data is compartmentalized based on classification and the need to know
- Model seeks to eliminate covert channels

- Model ensures that information always flows from a low security level to a higher security level and from a high integrity level to a low integrity level
- Whatever component directly affects the flow of information must dominate all components involved with the flow of information

Lattice Model

- Model consists of a set of objects constrained between the least upper bound and the greatest lower bound values.
- The least upper bound Is the value that defines the least level of object access rights granted to a subject
- The greatest lower bound is value that defines the maximum level of object access rights granted to a subject
- The goal of this model is to protect the confidentiality of an object an and only allow access by an authorized subject.

Non-interference model

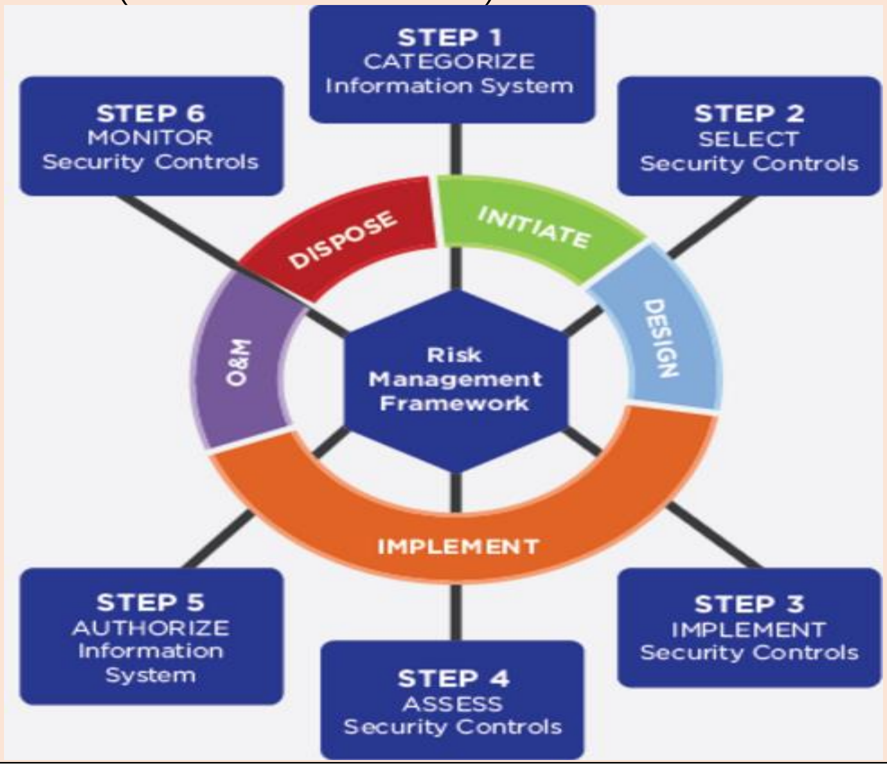
- TIP: think “what happens in Vegas stays in Vegas”
- Model ensures that actions at a higher security level does not interfere with the actions at a lower security level.
- The goal of this model is to protect the state of an entity at the lower security level by actions at the higher security level so that data does not pass through covert or timing channels.

3. Evaluation Criteria

- **TCSEC**
  - Trusted Computer System Evaluation Criteria (orange book)
    - Trust vs. assurance
    - D minimal protection
    - C1, C2 discretionary protection
    - B1, B2, B3 mandatory protection
    - A1 verified protection
  - ITSEC [introduced by Europe]
    - Function vs. assurance
- **Common criteria (ISO 15408)**
  - best of TCSEC & ITSEC
  - protection profile
  - Target of evaluation
  - Security target
  - Security packages
  - EAL rating
- **CMMI** (Capabilities Maturity Model Integrated)
  - Evaluating software development
  - TIP: MNEUMONIC: I Really Don’t Mind Oranges -- IRDMO
  - Level 1: initiating: chaotic, heroic efforts needed from staff
  - Level 2: repeatable: beginning of project management awareness, processes are put in place
  - Level 3: defined: well defined processes put in place with organizational support
  - Level 4: managed: product and processes focused on quantitative understanding of quality
  - Level 5: optimized: continuous process improvement
  - *most orgs are content with being level 3

- **IDEAL Model** (Initiate, Diagnose, Establish, Action, Leverage)

Certification & Accreditation

- NIACAP
  - National information assurance certification and accreditation
  - Certification: technical evaluation of the security components of a system in a environment
  - NIACAP is designed to ensure that all National Security Systems meet the requirements for Certification & Accreditation
  - The main document is the system Security Authorization Agreement (SSAA). This document gets updated throughout the NIACAP process.
- DIACAP
  - DoD information assurance certification and accreditation
  - Certification/accreditation process for all DoD-owned and/or controlled information systems
  - Baseline DoD information assurance controls
  - Main document is a DIACAP Scorecard, POA&M (plan of Action and Milestones)
- RMF
  - Risk Management Framework: should be replacing both NIACAP & DIACAP as the standard framework
  - System Security Plan (SSP)
  - Statement of Records Notice (SORN)
  - Minimum Security Baseline (MSB)
  - POA&M (Plan of Action & Milestones)
  - 

4. Technical Project Management

- Project is defined as a temporary endeavor with the goal of producing a unique product service or result.
- Project management is the application of skills, knowledge, tools and techniques to meet the goals of the project
- The project management lifecycle consists of the following:
    - **Initiating**: getting the project authorized and approved and collection of information at a high level
    - **Planning**: providing direction for the projects and determining baselines
    - **Execution**: doing the work of the project – producing deliverables and collecting "actuals" – data that describes what has happened
    - **Monitoring and Controlling**: baselines vs. actuals (variance analysis); tracking
    - **Closing**: ringing the project to an orderly formalized end
- Key documents in Project Management
    - Project charter
    - PM plan
    - Scope statement
    - Work breakdown structure
    - Scope, schedule, and cost baselines
    - Stakeholder register
    - Risk register
    - Quality baseline
    - Schedule
    - Budget
    - Resource assignments
    - Gantt and PERT charts
    - Numerous others
- For information security program management, be familiar with:
    - Evaluation criteria
    - Cost/benefit analysis
    - Security architecture
    - Certification & accreditation
    - Technical project management

5. Architecture & Design: Intro

- An information system's architecture must satisfy the defined business and security requirements.
- Security should be built into an information system by deign
- When designing system architecture, security and business requirements need to be carefully balanced.
- Tradeoffs are involved in reaching a balance between security and business requirements.
- The requirements of an information system are driven by the security policy of the organization that will use the system.
- To incorporate the abstract goals of a security policy into an information system's architecture, you will need to use security models.
- A security model lays out the framework and mathematical models that act as security-related specifications for a system architecture

- The system architecture, in turn, is the overall design of the components – such as hardware, operating systems, applications, and networks – of an information system. This design should meet the specifications provided by the security model.

Architecture Components

- Enterprise architecture that is a representation of the mode of operation of an enterprise. This mode of operation needs to be derived systematically.
- Network architecture that describes how various entities in a network communicate with each other. It also defines if a system is an open system or a closed system.
- Platform architecture that describes how a system optimally uses system resources, such as storage devices, input/output (I/O) devices, memory management, CPU states, operating system, and various utilities.
- Protection mechanisms refer to the mechanisms needed to protect the system and ensure that all the objects in the system are separated.
- Security models refer to methods to integrate security into a system's architecture. Some common security models are Bell-LaPadula, Biba, and Clark-Wilson

*Security architecture is part of the overall architecture of an information system. It directs how the components included in the system architecture should be organized to ensure that security requirements are met. The security architecture of an information system should include:

- A description of the locations in the overall architecture where security measures should be placed
- A description of how various components of the architecture should interact to ensure security
- The security specifications to be followed when designing and developing the system.

6. Architecture & Design: Hardware

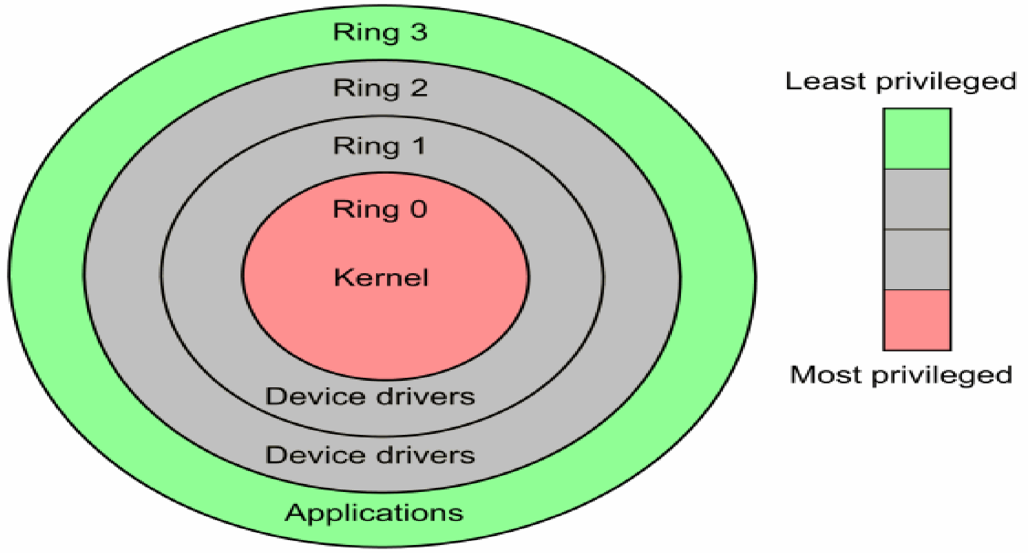
Computer Architecture

- It comprises all the parts in a computer system that are necessary for it to function. Such parts include the operating system, memory chips, logic circuits, storage devices, I/O devices, security components, buses, and networking components.
- **The Central Processing Unit** (**CPU**) – processes the instructions provided by the various application/programs. To do this the CPU needs to access such instructions from their memory locations.
- The CPU can access the memory locations in its cache, along with memory locations in the **random access memory** (**RAM**). These types of memory are called primary memory.
- The major components:
  - The **arithmetic logic unit** (**ALU**) – the brain of the CPU
  - **Control unit** (coordinates instruction execution in and out of RAM)
  - **Registers** that act as temporary memory locations and store the memory addresses of the instructions and data that needs processing by the CPU. (waiting room for CPU, information waiting to be processed)
- **Program**: an application
- **Process**: a program loaded into memory
- **Thread**: each individual instruction within a process
- **Multiprogramming**: no true isolation, enables multitasking (more than 2 programs at the same time)

- **Multiprocessing:** more than one CPU (multiple units of code running at the same time)
- **Multithreading:** in the past multiple CPUs were needed. Today multi-core processors provide this.
- **Operating System Architecture**
- **Process Activity**
- **Memory Management**
- **Memory Types: RAM, ROM, etc**.
- **Virtual Memory**
- **CPU Modes & Protection Rings**

7. Architecture & Design: CPU Modes & Protection Rings

- **Protection Rings** provide a security mechanism for an operating system by creating boundaries between the various processes operating on a system and ensures that processes do not affect each other or harm critical system components.
- **Ring 0 –** operating system kernel (supervisor/privilege mode)
- **Ring 1 –** remaining parts of the operating system (OS)
- **Ring 2 –** operating system and I/O drivers and OS utilities
- **Ring 3 –** applications (programs) and user activity



-
- *outer layer cannot access inner layer without an interface; inner layer can access everything outer.
- Protection mechanisms
  - TIP: think of processes as kids and how then want attention, how do you effectively divide that attention with the right resources.
  - Domain
  - Layering & data hiding
  - Virtual machines
    - A virtual machine is a simulated real machine environment created to simultaneously run multiple applications on a computer.
  - Additional storage devices
  - Input / output device management

System Architecture

- Defined subset of subjects and objects

- Trusted Computing Base (TCB)
- Security perimeter
    - It delineates the trusted and the untrusted components within a computer system.
- **Reference Monitor** (the law)
    - This reference monitor is an abstract machine concept that mediates all access between subjects and objects.
- **Security Kernel** (the police that enforce the law)
    - The security kernel enforces the reference monitor concept:
        - Must facilitate isolation of processes
        - Must be invoked at every access attempt
        - Must be small enough to be tested and verified in comprehensive manner
- Security policy – a set of rules on how resources are managed within a computer system

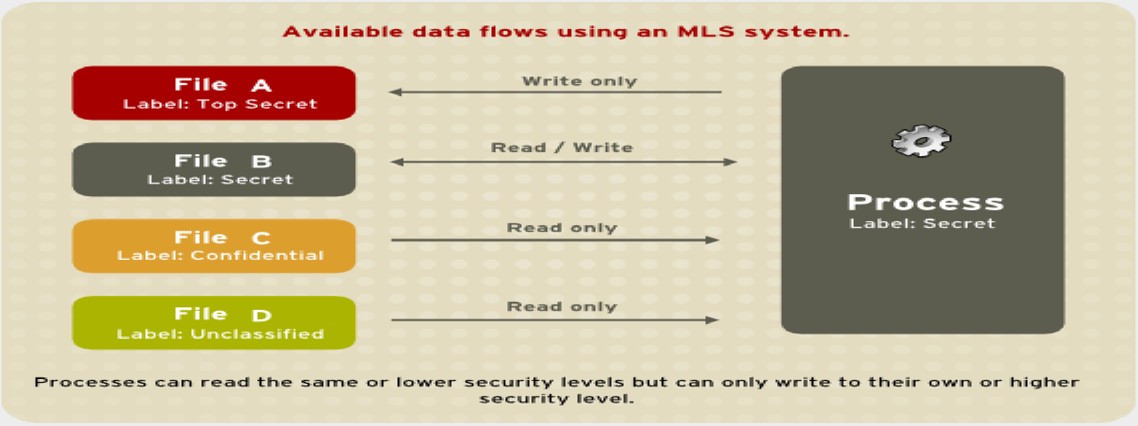
Security Models

- The function of a security model is to:
    - Map the abstract goals of a security policies to an information system.
    - Specify mathematical formulae and data structures for implementing security policy goals.
- While a security policy states goals without specifying how to accomplish them, a security model specifies a framework to implement these goals.
- An organization can use different types of security models. However, it is very important for security personnel to understand the different security models to protect the organization’s resources.
- For example; the security model that a military organization uses is quite different from that of a commercial entity, due to the variations in the types of data.
- Security model can be formal when it is based on pure mathematical implementation of security policies and assure high security. For example, in military systems, air controller systems, etc.
- Security Model is informal when it merely describes how to express and execute security policies.

8. Architecture & Design: Integrity Models

***models are used to architect secure systems**

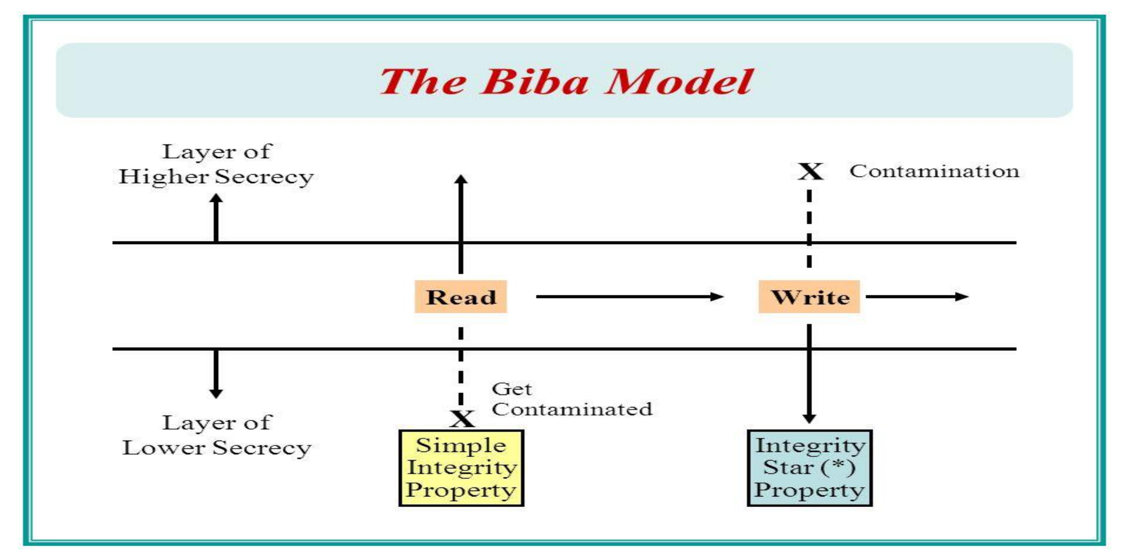
Bell-LaPadula Model



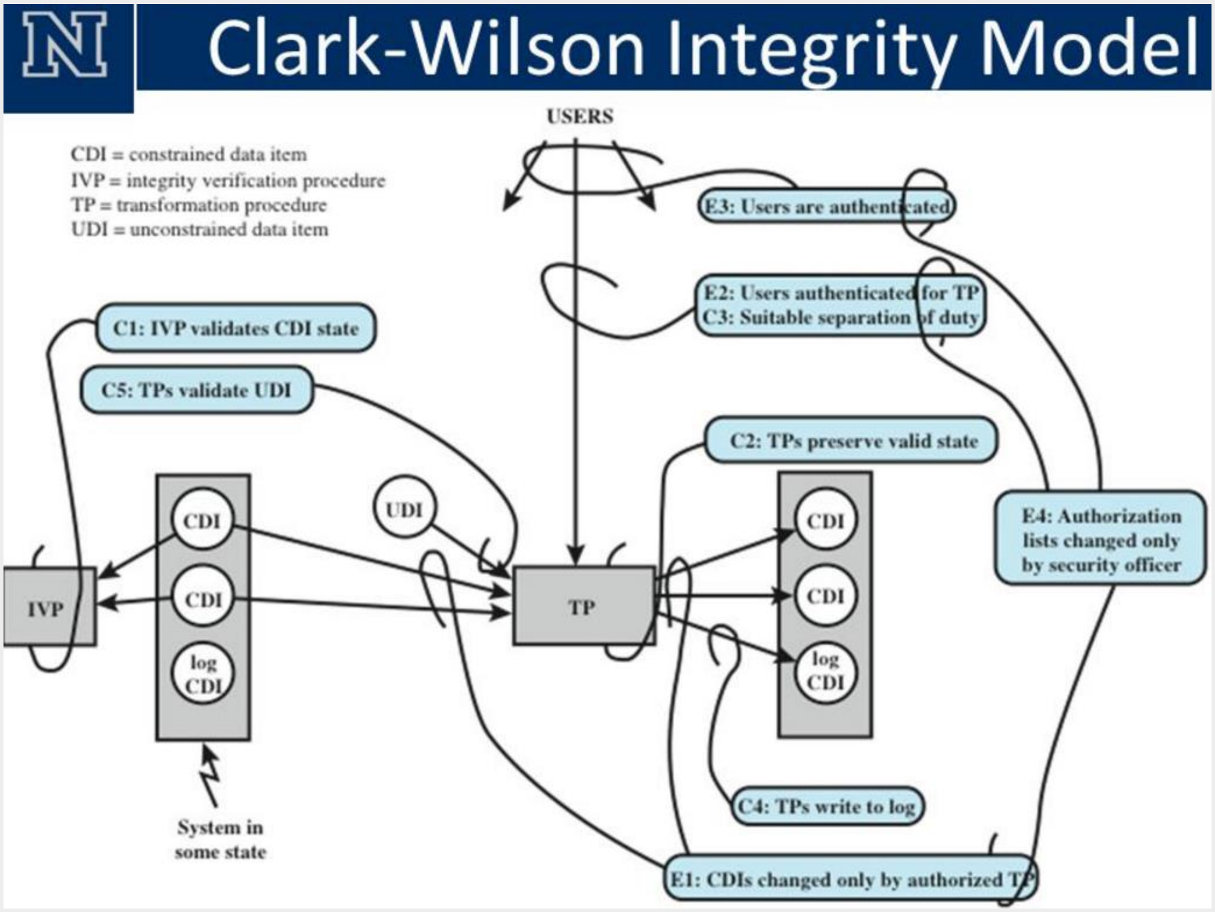
Available data flows using an MLS system.

Processes can read the same or lower security levels but can only write to their own or higher security level.

Biba Model



Clark-Wilson Model


Clark-Wilson Integrity Model
USERS
CDI = constrained data item
IVP = integrity verification procedure
TP = transformation procedure
UDI = unconstrained data item
E3: Users are authenticated
E2: Users authenticated for TP
C3: Suitable separation of duty
C1: IVP validates CDI state
C5: TPs validate UDI
C2: TPs preserve valid state
E4: Authorization lists changed only by security officer
IVP
CDI
CDI
log CDI
UDI
TP
CDI
CDI
log CDI
System in some state
C4: TPs write to log
E1: CDIs changed only by authorized TP

8. Architecture & Design: Evaluation Criteria

Why Evaluate?

- To carefully examine the security-related components of a system
- Trust vs. assurance

- The orange book (TCSEC) – old
  - Designed to just address confidentiality of a system
  - Based on Bell-LaPadula model
  - Uses a hierarchically ordered series of evaluation classes (the lower the number, the less secure)
    - A1 – verified protection
    - B1, B2, B3 – mandatory protection
    - C1, C2 – discretionary protection
    - D – minimal security
- The orange book & the rainbow series
- ITSEC (information technology security evaluation criteria)
- Common criteria
- RMF (risk management framework) – becoming the modern standard

9. Architecture & Design: Assurance

- Trust tells us function of the system.
- Assurance tells us the reliability of the process.
- Evaluation criteria are used to determine trust (function) and assurance.

Common Criteria (CC)

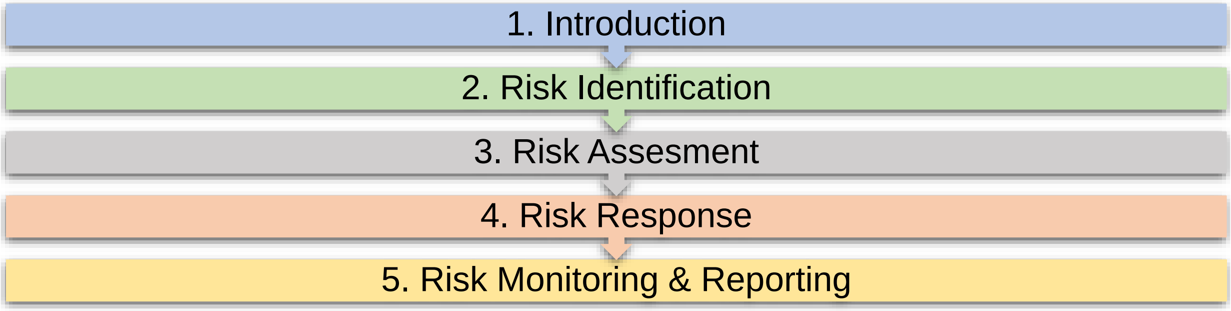
- ISO (15408) Standard created in 1993 for global security evaluation
- Made up from TCSEC, ITSEC, and the Canadian version
- Components:
- Protection Profile – a set of security requirements and objectives for the system
- A protection profile consists of:
  - Descriptive elements – contains the name of the profile and the description of the security problem to be solved.
  - Rationale – justifies the profile and provides a detailed description of the real-world problems that need to be solved.
  - Functional requirement – establishes a protection boundary that the product must provide
  - Development assurance requirements – identify the requirements for the various phases of the product
  - Evaluation assurance requirements – establish the type and intensity of the evaluation
- Common criteria ratings (EAL)
  - EAL (evaluation assurance level) 1-7
    - 1 – functionally tested
    - 2 – structurally tested
    - 3 – methodically tested and checked
    - 4 – methodically designed, tested, and reviewed
    - 5 – semi formally designed and tested
    - 6 – semi formally verified designed and tested
    - 7 – formally verified designed and tested
  - Overview:
    - Client produces a protection profile that's their list of requirements
    - Vendors provide a target of evaluation, which is a system to meet those requirements as well as a security target that details how the requirements and protection will be met.
    - The vendor may include other evaluation packages

        - Then submitted for 3rd party audit; the auditor identifies both trust (functionality) and assurance and assigns an EAL rating
- Ideally, we look towards certification & accreditation before putting a system in place
- Once a product passes certification, it goes through accreditation – if approved my management, then the product is chosen / implemented.

10. Architecture & Design: Review

- For system architecture & design, understand the core concepts of:
    - Elements of system architecture
    - Protection mechanisms
    - Security kernel and reference models
    - Security models
    - Evaluation criteria
- All of this ensures the secure design of a system.

II. RISK MANAGEMENT FRAMEWORK:


1. Introduction
2. Risk Identification
3. Risk Assesment
4. Risk Response
5. Risk Monitoring & Reporting

1. Introduction

Governance vs. Management

- **Governance**:
    - Are we doing the right things?
    - Are we doing things right?
    - Are we getting things done well?
    - Are we maximizing the benefits?
- **Management**: planning, building, running and monitoring per the directions established and in compliance to governance.

Definitions

- **Asset**: any item of value to the organization
- **Vulnerability**:
    - Internal weakness
    - External lack of protection
- **Threat**: a negative risk event that threatens an objective
- **Risk**: the likelihood of a threat compromising an asset
- **Risk management**: activities implemented to direct and control an enterprise in relation to risk
- **Probability**: the likelihood of an event
- **Impact**: how much will the output be affected?
- **Secondary risk**: created when one risk response created another risk event

- **Residual risk**: after a risk response is applied, residual risk is what remains
- Remember, our goal is not to eliminate all risks, but to effectively address them

IT Risk

- IT security is based on risk management approach
- Risk = Probability * Impact
- Identify and valuate assets, identify and valuate threats, find a cost-effective solution
- Continue to monitor risks and review periodically or in the event of a risk change
  - **Control risk**: controls are chosen to mitigate risk, but if incorrect controls are chosen, configured incorrectly, or if it does not work properly, the control will fail.
  - **Project Risk**: much work within IT is managed as a project. Identifying risks early and often increase the chance of a project being successful.
  - **Change risk**: few environments are static. As technology or the environment changes, new risks appear.

IT Risk Management:

- Implements a risk strategy as defined by governance and is indicative of the culture, appetite and tolerance. It will consider the technology and budget (cost/benefit analysis) and addresses compliance with corporate policy.
- A cyclical process of Risk Identification, Risk Assessment, Risk Mitigation, and Ongoing Monitoring
- Failure to perform anyone of these elements will leave an organization vulnerable

Sources of IT Risk:

- Insider threats
- Outsider threats
- Hardware failures
- Resource failure
- Vendors
- Changing environment
- Many others

Benefits of Risk Management:

- Better oversight of organizational assets
- Minimizing loss
- Identification of threats, vulnerabilities, and risks
- Prioritization of risk responses
- Legal and regulatory compliance
- Increased likelihood of project success
- Increased confidence of customers and shareholders
- Better incident management
- Better ability to meet business objectives

The Relationship of Business Continuity & Risk Management

- Risk management is usually a precursor to Business continuity
- Risk deals more closely with high to medium likelihood events
- **Business continuity** tends to deal with events that have a lower likelihood, but have a high impact
- Business continuity is a “safety net” under risk management

IS Audit

- **IS audit** providing the assurance to management of the effectiveness of the IS controls in place, IT Risk management and compliance
- Part of due diligence
- Methodical and structured review to validate compliance

Gap Analysis

- **Determine desired position**
  - Business objectives
  - Laws and regulations
- **Determining current position**
  - Internal audits
- **Close the Gap**
  - Prioritize based on business and risk

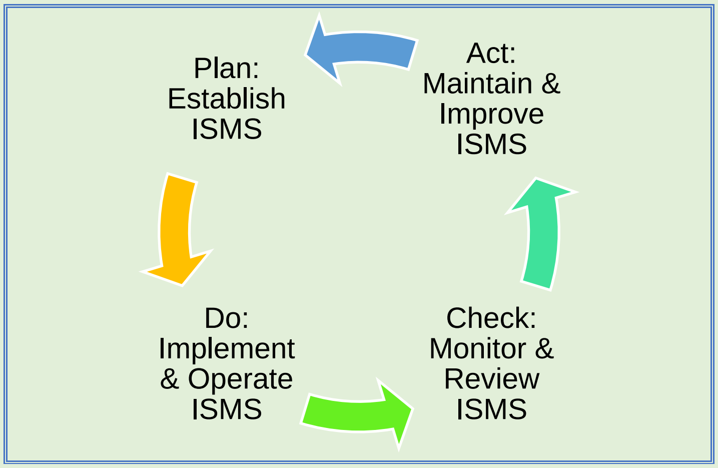
2. Risk Identification

- Identify relevant standards and frameworks and practices
- Apply risk identification techniques
- Distinguish between threats and vulnerabilities
- Identify relevant stakeholders
- Discuss risk scenario development tools and techniques
- Key risk management concepts
- Risk registers
- Risk awareness

Risk Management Frameworks:

- COBIT 5 for RISK
- COSO (Committee for Sponsoring Organizations of the Treadway Commission
- ISO Standards 27005
- NIST SP 800-30 Guide for Conducting Risk Assessments
- NIST SP 800-39 Managing Information Security Risks

PLAN-DO-CHECK-ACT Model:


Plan: Establish ISMS
Act: Maintain & Improve ISMS
Do: Implement & Operate ISMS
Check: Monitor & Review ISMS

Capability Maturity Model Integration

- Carnegie-Mellon Software Engineering Institute (SEI)
- A process improvement maturity model for development of products and services

ISO 27005 Information Security Risk Management

- Risk context, assessment, identification, analysis, evaluation, treatment, acceptance, communication & consultation, monitoring and review

- **Risk Context**
    - Set the criteria for information security management (criticality, scope, boundaries)
    - Determine company's philosophy toward risk
    - Look at regulatory and legislative drivers
    - Look at existing frameworks in place (ISO 9000, Six sigma, CMMI)
    - Establish an appropriate cross-functional group to the risk assessment
- **Risk Assessment**
    - Identify assets
    - Valuate assets
    - The valuation of your assets will drive the amount you will spend to protect them. Use the expertise of your management staff or outsource this skill for accurate estimates.
- **Risk Identification**
    - Look at your assets in terms of: vulnerabilities, threats, existing controls and their effectiveness, impact
- **Risk Analysis**
    - Probability, Impact, Qualitative Analysis, Quantitative analysis
- **Risk Evaluation**
    - Comparing probability and impact of risks to risk criteria
    - Prioritizing risk elements
    - Identifying risk triggers
- **Risk Treatment**
    - **Risk modification:** reduce the probability and/or the impact of a risk
    - **Risk retention:** sometimes with research it is determined that it is cheaper to pay the costs over time, than transfer a risk. EX: Insurance deductibles
    - **Risk avoidance:** don't attempt the action as the risk is too high
    - **Risk sharing or transference:** Insurance or SLAs
    - **Risk acceptance:** when the cost of the countermeasure is greater than the potential for loss, it may be smart to accept the risk.

A Risk Management Program Should be…

- Comprehensive and complete
- Auditable
- Justifiable
- Legal
- Monitored
- Enforced
- Up to date
- Managed

Methods to Identify Risks

- **Investment risk**: will the investment in IT services and controls pay off?
- **Access** or **security risk**: unauthorized access to system resources?
- **Disclosure risk**: breach in confidentiality
- **Integrity risk**: modification of data
- **Relevance risk**: not getting the right information to the right people at the right time
- **Availability**: timely access to resources
- **Infrastructure risk**: is the current environment capable of meeting the business objectives and goals for the organization
- **Project risk**: will IT projects meet their goals

- *Utilize a risk register

IT Strategy of the Business

- Drives the IT Risk Strategy
- Buy-in from and active support from senior management
- Alignment with Business Goals & Objectives necessary to prioritize risk responses to those areas with least tolerance for loss.
- Risk management centrally managed as an enterprise wide position (Chief Risk Officer)

The Role of InfoSec within an Organization

- Priority is to support the mission of the organization
- Require judgement based on risk tolerance of organization, cost and benefit
- Role of the security professional is that of a risk advisor, not a decision maker

Best Practices (To Protect C-I-A)

- Separation of Duties (SOD)
- Mandatory vacations
- Job rotation
- Least privilege
- Need to know
- Dual control

Knowledge Transfer

- Awareness, Training, Education
- Usually, the weakest link in any organizational security policy are the people within the organization
- Loss is not always caused by malicious behavior
- The ultimate goal of knowledge transfer is to modify employee behavior

Explaining How and Why

- **Security Awareness Training:**
  - Employees cannot and will not follow the directives and procedures, if they do not know about them
  - Employees will often find another mans of performing an action when their desired activity is blocked. Help them understand why we do what we do.
  - Employees must know expectations and ramifications, if not met
  - Employee recognition award program
  - Part of due care (action); (due diligence is research)
  - Administrative control
- Overriding benefits:
  - Modifies employee behavior and improves attitudes towards information security
  - Increases the ability to hold employees accountable for their actions
  - Raises collective security awareness level of the organization
- Implementation
  - Avoid one-size-fits-all training
  - All users should go through basic security awareness training
  - Technicians/administrators should attend more technically focused
  - Managers should attend IT risk training

3. Risk Assessment

- Risk assessment is the process used to identify and valuate a risk event.

Risk Identification vs Risk Assessment

- **Identification** has a focus on determining and documenting the types of risks that can affect an organization. We enumerate risks in identification
- **Assessment** is a means of evaluating the risk and its potential affect. Usually, we look to learn a risk value from assessment

NIST 800-100 Risk Assessment:

1. **System characterization**
    - What is the use for them system?
    - What classification of data does the system hold?
    - What impact would result if the system became compromised?
2. **Threat identification**
3. **Vulnerability identification**
4. **Control analysis**
    - Probability: how likely an event is to occur
    - Impact: how much damage will be done
    - Risk Value:
        - **Qualitative Analysis**:
            - Subjective
            - Opinion based
            - SME's are often queried using the Delphi method
            - Used to identify and start to prioritize risks
            - This MUST come before Quantitative Analysis
            - Probability and impact matrix is often used
        - **Quantitative Analysis**:
            - Objective, fact-based
            - Requires more skill and expertise
            - Business decisions should be made on quantitative analysis
            - Is the basis for cost/benefit decisions?
        - Quantitative analysis Formulas & Definitions:
            - (**AV**) **Asset Value**: dollar figure that represents what the asset is worth to the organization
            - (**EF**) **Exposure Factor**: the percentage of loss that is expected to result in the manifestation of a risk event.
            - (**SLE**) **Single Loss Expectancy**: dollar figure that represents the cost of a single occurrence of a threat instance
            - (**AR**) **Annual Rate of Occurrence**: how often the threat is expected to materialize
            - (**ALE**) **Annual Loss Expectancy**: cost per year because of the threat
            - **(TCO) total cost of ownership**: the total cost of implementing a safeguard. Often in addition to initial costs, there are ongoing maintenance fees as well.
            - **(ROI) Return on Investment**: amount of money saved by implementation of a safeguard. Sometimes referred to as the value of the safeguard/control.
            - **SLE = AV * EF**
            - **ALE = SLE * ARO**
            - **TCO = Initial cost of control + yearly fees**
            - **Return on Investment:**

        - ALE (before implementing control)
        - - ALE (after implementing control)
        - - cost of control
        - = ROI (Value of Control)

5. Control Recommendations
    - Cost/benefit analysis
    - How much security is enough? (JUST ENOUGH)
    - What helps us make these decisions?
6. Documentation

Results Documentation

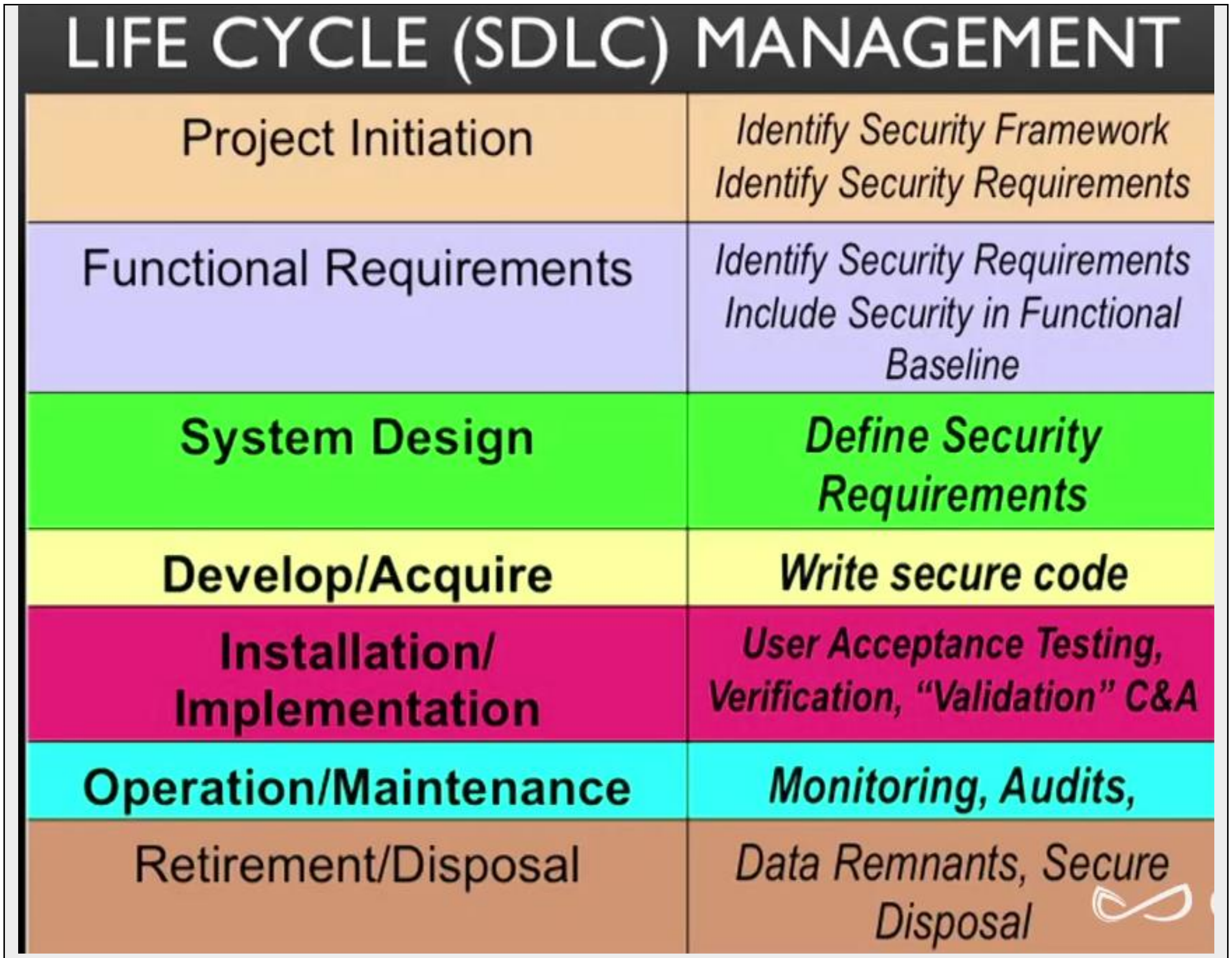
- Risk register
- Probability and Impact matrix (temperature matrix)
- EMV (expected monetary value) analysis
- Decision tree analysis
- Ishakawa / fishbone (cause & effect) diagram
- Delphi technique

Information Security Controls

- Understand the categories of controls
- Control administration
- Identity management controls
- Cryptographic controls
- Network access controls
- Testing controls
    - Vulnerability assessment
    - Penetration testing
- Best approach is a layered defense!

Control categories

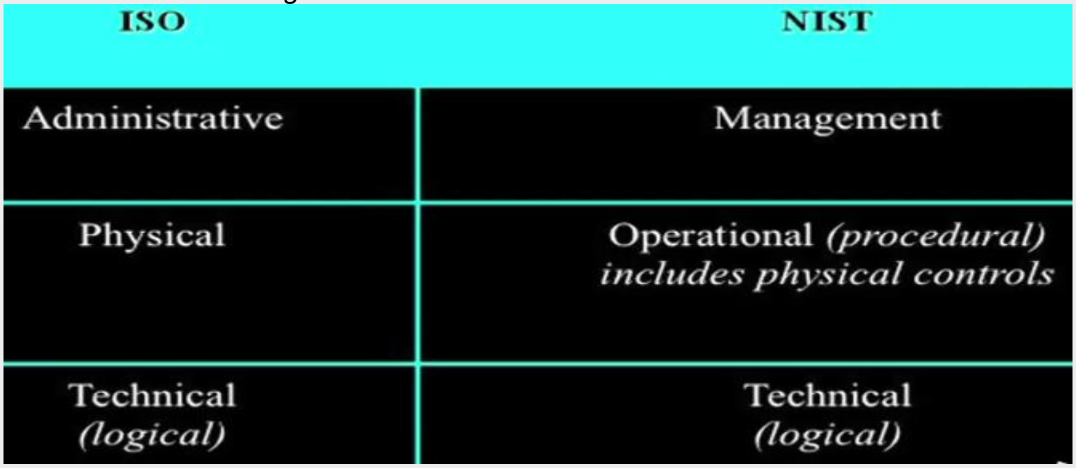
- Preventive (gate, fence)
- Deterrent (lighting, signs)
- Corrective (quarantine)
- Detective (audit logs)
- Directive (employee handbooks)
- Compensating
- Recovery (data backups, RAID)
- *Controls can present a considerable risk if they are not configured properly or if they fail



LIFE CYCLE (SDLC) MANAGEMENT

Project Initiation	*Identify Security Framework* *Identify Security Requirements*
Functional Requirements	*Identify Security Requirements* *Include Security in Functional Baseline*
System Design	***Define Security Requirements***
Develop/Acquire	***Write secure code***
Installation/ Implementation	***User Acceptance Testing, Verification, "Validation" C&A***
Operation/Maintenance	***Monitoring, Audits,***
Retirement/Disposal	*Data Remnants, Secure Disposal*

ISO and NIST Control Categories



ISO	NIST
Administrative	Management
Physical	Operational *(procedural) includes physical controls*
Technical *(logical)*	Technical *(logical)*

Layered Defense (defense in depth)

- Policies
- Firewalls
- IDS/ IPS
- Router / Switch
- Application
- Middleware
- Operating system
- Other hardware

Enterprise Risks: Hardware

- Outdated
- Poorly maintained
- Misconfigured hardware
- No configuration management
- Poor asset control
- Physically accessible
- Unauthorized hardware

Enterprise Risks: Hardware

- Logic flaws
- Unpatched systems
- Disclosure of sensitive information
- Improper access control
- Loss of source code
- Lack of bounds checking
- Lack of input validation

Enterprise Risk: Databases

- Code injection
- Scripting
- Aggregation
- Inference
- Entity, semantic, and referential integrity

Enterprise Risks: Utilities

- Power
  - Spikes
  - Surge
  - Sag
  - Brownout
  - Fault
  - Blackout
- HVAC (heating, ventilation, air-conditioning)
- Humidity
- EMI (electromagnetic interference)
- RFI (radio frequency interference)

Enterprise Risks: Network Components

- Cable
- Hubs
- Switches
- Routers
- Firewalls

- Proxies
- Network services
- Wireless communication

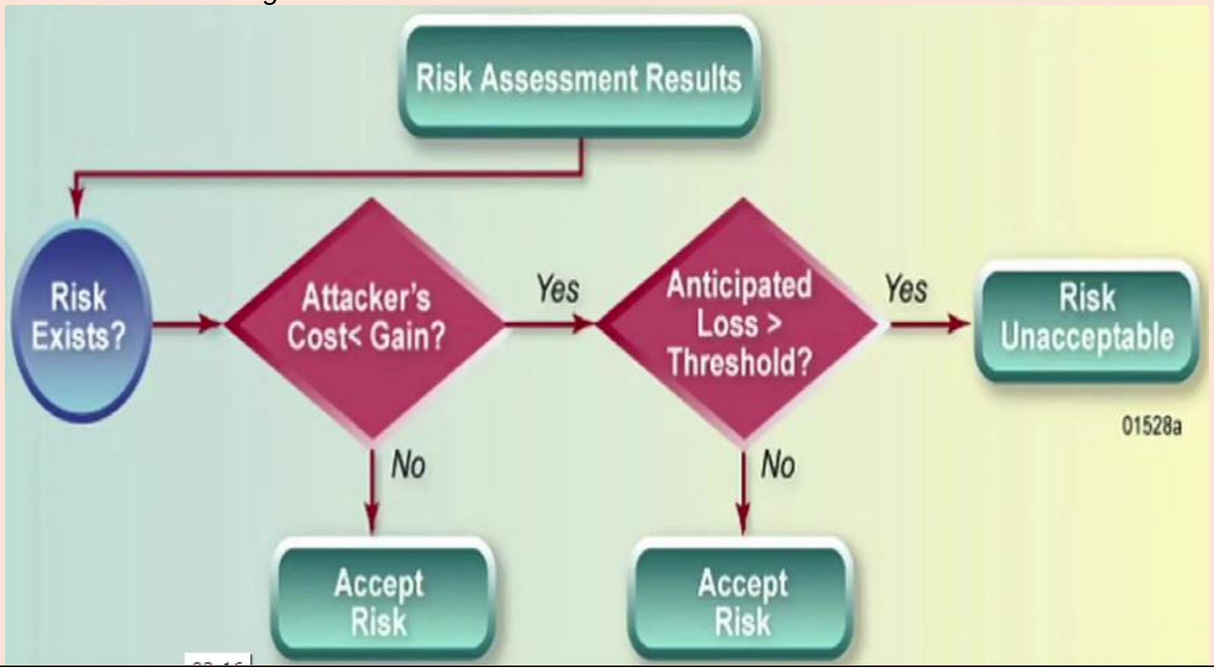
Enterprise Risk: Users

- Internal theft
- Fraud
- Salami attacks
- Data diddling
- Falsification of timesheets
- Compromise of sensitive information
- Disgruntled employees

4. Risk Response / Mitigation

- **Risk Response**: to determine risk strategies and evaluate their effectiveness to manage risk to a level in alignment with business objectives
- **Risk response strategies:**
    - Reduce (risk avoidance)
    - Transfer
    - Accept
- Risk reduction through:
    - Policies
    - Technology
- When risk management fails…business continuity saves the day!
- *Risk management should always be dependent on cost/benefit analysis

SP800-100 Risk Mitigation:



Risk Reduction

- Lesson the probability and/or impact of a risk event
- Sometimes referred to as risk mitigation
- A very frequent response to risk
- Remember, we don't usually think about risk elimination, usually we strive to reduce risk to acceptable levels
- *The ultimate risk reduction is risk avoidance

Risk Transference

- Sharing the potential for loss with someone else
  - Insurance
  - Service level agreements
  - Contract modification
- *Transference doesn't lessen the probability or impact of the risk. It simply decreases your share of the loss.

Risk Acceptance

- When the cost of the countermeasure is greater than the potential for loss, one may choose to accept the risk
- True risk acceptance requires due diligence and proof that this is a good decision, to be less likely to be liable for damages

Risk Mitigation Through Policies

- **Separation of Duties**: prevents any one person from becoming too powerful within an organization. This policy also provides singleness of focus. For instance, a network admin who is concerned with providing users access to resources should never be the security admin. This policy also helps to prevent collusion as there are many individuals with discrete capabilities. Separation of duties is a preventative control.
- **Dual Control**: requiring more than one user to perform a task. M of N control, and split knowledge are types of dual control.
- **Mandatory Vacation**: prevents an operator from having exclusive use of a system. Periodically that individual is forced to take a vacation and relegate control of the system to someone else. This policy is a detective control.
- **Job rotation**: similar in purpose to mandatory vacations, but with the added benefit of cross-training employees.
- **Least privilege:** allowing users to have only the required access to do their jobs.
- **Need to know**: in addition to clearance, users must also have "need to know" to access classified data
- **Strong configuration management/change control policies** are important to promote network and system stability.
- **Acceptable Use Policies:** alert users as to how company resources are to be utilized
- **Data classification policy:** provides guidance on requirements for the classification of materials and other guidelines related to baseline security
- **Data Privacy:** details how sensitive information is to be protected
- **Computer ownership:** addresses who owns company issued computers/laptops/devices, etc.
- **Data ownership:** addresses who owns the data that the company works with. For instance, is a patient the owner of his healthcare record, or is it the hospital?

Risk Mitigation through Technology

- **Access Control**
  - IAAA

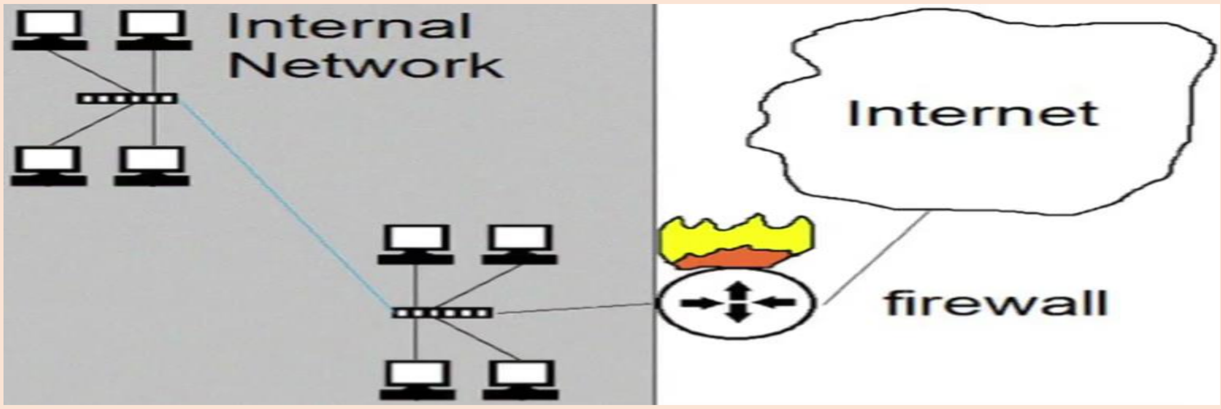
    - Centralized vs Decentralized
- **Network devices**
    - Firewalls
    - IDS/IPS
    - Audit logs
    - Honeypots/honeynets
- **Cryptography**

Access Control

- Access is the data flow between a subject and an object.
    - Subject Is active – a person, process, or program,
    - Object is passive – a resource (file, printer, etc.)
    - Access control should support the CIA triad and regulate what a subject can do with an object
- IAAA of access control:
    - **Identification**: make a claim (user ID etc.)
        - public information (usually we aren't concerned with protecting identities)
        - identification must be unique for accountability
        - standard naming schemes should be used
        - identifier should not indicate extra information about user (like job position)
            - User ID, Account #, RFID, IP or MAC address
    - **Authentication**: provide support (proof) for your claim
        - Proving your identity:
            - Type 1: something you know
                - Passwords/passphrases/cognitive password
            - Type 2: something you have
                - Token, card, certificate, cookies, cryptographic key
            - Type 3: something you are
                - Biometrics
    - **Authorization**: what rights and permissions you have
        - Utilize principle of least privilege and need to know
    - **Auditing**: accountability – matching actions to subject
        - internal audit of control objectives, controls, processes and procedures of its ISMS:
            - conform to the requirements of this international standard and relevant legislation or regulations
            - conform to the identified information security requirements
            - are effectively implemented and maintained
            - perform as expected
        - management review
        - general
            - defining review policy
            - schedule at least once a year or as risks change
        - inputs
            - audits
            - other stakeholder feedback
        - outputs
            - improvement plans
            - other remediation

        - Gap analysis
            - Determine desired position
            - Business objectives
            - Laws and regulations
        - Determining current position
            - Internal audits
        - Close the gap
            - Prioritize based on business and risk

Network Devices: Firewalls



- **Firewalls enforce network policy**
- Usually firewalls are put on the perimeter of a network and allow or deny traffic based on company or network policy
- Must have IP forwarding turned off*
- Firewalls are often used to create a DMZ.
- Generally, are dual/multi homed* (have multiple interfaces)
- Types of firewalls:
    - **Packet filtering**
        - Uses access control lists (ACLs), which are rules that a firewall applies to each packet it receives
        - Not stateful, just looks at the network and transport layer packets (IP addresses, ports, and "flags")
            - Does not look in the application, cannot block viruses, etc.
            - Generally, does not support anything advanced or custom
    - **Stateful**
        - Router keeps track of connections in a table. It knows which conversations are active, who is involved etc.
        - It allows return traffic to come back where a packet filter would have a specific rule to define returned traffic
        - More complex, and can launch DoS against by trying to fill up all the entries in the state tables/use up memory.
        - If rebooted, can disrupt conversation that had been occurring
        - Context dependent access control*
    - **Proxy**
        - Two types or proxies
            - Circuit level
            - Application

        - both types of proxies hide the internal hosts/addressing from the outside world
    - **Dynamic packet filtering**
- Firewalls can be used to create a **DMZ**
    - A DMZ (demilitarized zone) is a buffer zone between an unprotected network and a protected network that allows for the monitoring and regulation of traffic between the two.
        - Internet accessible servers (bastion hosts) are placed in a DMZ between the internet and internal network
- **NAT/PAT**
    - a proxy that works without special software and is transparent to the end users.
    - Remaps IP addresses, allowing you to use private addresses internally and map them to public IP addresses
    - NAT (network address translation) allows a one-to-one mapping of IP addresses
    - PAT port address translation) allows multiple private addresses to share one public address

Cryptography

- Plain text + initialization vector + algorithm + key = CIPHERTEXT
- **Plain text** Is unencrypted text
- **Initialization vector** (**IV**) adds randomness to the beginning of the process
- **Algorithm** is the collection of math functions that can be performed
- **Key**: instruction set on how to use the algorithm
- **Symmetric cryptography**
    - Symmetric = same
    - In symmetric cryptography, the same key is used to both encrypt and decrypt
    - Very fast means of encrypting/decrypting with good strength for privacy
    - Proffered means of protecting privacy data
    - Also, can be called “Private Key” “Secret Key” or “Shared Key”
- Drawbacks to symmetric cryptography
    - Out of band key exchange
    - Not scalable
    - No authenticity, integrity, or non-repudiation
- **Asymmetric cryptography**
    - Every user has a key pair
        - Public key is made available to anyone who requests it
        - Private key is only available to that user and must not be disclosed or shared
    - The keys are mathematically related so that anything is encrypted with one key can only be decrypted by the other
- **Hybrid cryptography in SSL/TLS**
    - Client initiates a secure connection
    - Server responds by sending its public key to the client
    - The client then generates a symmetric session key
    - Client encrypts uses the server’s public key to encrypt the session key
    - Client sends the session key (encrypted with the server’s public key) to the server
    - Server uses its private key to decrypt the session

    - Now that a symmetric session key has been distributed, both parties have a secure channel in which to communicate.

Integrity

- Data gets modified
- Accidentally through corruption
- Intentionally through malicious alteration
- **Hash**: only good for accidentally modification
- **MAC**: provides reasonable authenticity and integrity not strong enough to be non-repudiation (because it uses a symmetric key)
- **Digital signatures**: can detect both malicious and accidental modification, but requires an overhead. Provides true non-repudiation.

Hashing

- Digital representation of the contents of the file, aka message digest
- If the file changes, the hash will change
- One way math
- When two different documents produce the same hash, it is called a collision
- A birthday attack is an attempt to cause collisions. It is based on the idea that it is easier to find two hashes that happen to match than to produce a specific hash.

Digital Signature

- Message is hashed
- Hash is encrypted by sender's private key
- **SHA-1** is generally used for that hash
- **RSA** is the asymmetric encryption algorithm that encrypts the hash with the sender's private key

Certificates

- X.509 v.4 standard
- Provides authenticity of a server's public key
- Necessary to avoid MITM attacks with server's using SSL or TLS
- Digitally signed by Certificate Authority (CA)

PKI (Public Key Infrastructure)

- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Repository
- Certificate Revocation List

Business Continuity and Disaster Recovery Planning

- **Business Continuity Planning**: focusing on sustaining operations and protecting the viability of the business following a disaster, until normal business conditions can be restored. The BCP is an "umbrella" term that includes many other plan including the DRP. Long term focused.
- **Disaster Recovery Planning**: goal is to minimize the effects of a disaster and to take the necessary steps to ensure that the resources, personnel and business processes can resume operations in a timely manner. Deals with the immediate aftermath of the disaster, and if often IT focused. Short term focused.
- Mitigate risks
    - Reduce negative effects:
        - **Life Safety** is the NUMBER 1 PRIORITY

        - **Reputation**: the second most important asset of an organization. Though specific systems are certainly essential, don't forget to focus on the big picture – protect the company as a whole

Business Continuity Planning

- Disaster recovery and continuity planning deal with uncertainty and chance
    - Must identify **all possible threats** and estimate possible damage
    - Develop viable alternatives
- **Threat types**:
    - Man-Made: strikes, riots, fires, terrorism, hackers, vandals
    - Natural: tornado, flood, earthquake
    - Technical: power outage, device failure, loss of a T1 line
- **Categories of disruptions**
    - Non-disaster (incident)
        - Disruption of service
        - Device malfunction
    - Emergency/crisis
        - Urgency, immediate event where there is the potential for loss of life or property
    - Disaster
        - Entire facility unusable for a day or longer
    - Catastrophe
        - Destroys facility
    - A company should understand and be prepared for each category
- *ANYONE CAN DECLARE AN EMERGENCY, ONLY THE **BCP COORDINATOR** CAN DECLARE A DISASTER
- **ISO 27031 –** framework for business continuity planning

Business Continuity Plan: Sub Plans

- **BRP** (Business Recovery Plan)
    - Purpose: provide procedures for recovering business operations immediately following a disaster
    - Scope: addresses business processes; **not IT-focused**; IT addressed based only on its support for business process
- **COOP** (Continuity of Operations Plan)
    - Purpose: provide procedures capabilities to sustain an organization's **essential**, strategic functions at an alternate site for up to 30 days.
    - Scope: addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
- **Continuity of Support Plan/IT Contingency Plan**
    - Purpose: provide procedures and capabilities for recovering a **major** application or general support system
    - Scope: same as IT contingency plan; addresses IT system disruptions; not business process focused
- **Crisis Communication Plan**
    - Purpose: provides procedures for **disseminating** status reports to personnel and the public
    - Scope: addresses communications with personnel and the public; not IT focused
- **Cyber Incident Response Plan**

  - Purpose: provides strategies to **detect**, **respond** to, and **limit consequences** of malicious cyber intent
  - Scope: focuses on information security responses to incidents affecting systems and/or networks
- **DRP** (Disaster Recovery Plan)
  - Purpose: provide detailed procedures to **facilitate recovery** of capabilities at an alternate site
  - Scope: **often** IT-focused; limited to major disruptions with long-term effects
- **OEP** (Occupant Emergency Plan)
  - Purpose: provide coordinated procedures for minimizing **loss of life** or **injury** and protecting property damage in response to a physical threat
  - Scope: focuses on **personnel and property** to the specific facility; not business process or IT system functionality based. May also be referred to as Crisis or Incident Management plans. However, the OEP concept should be recognizable as the **"initial response to the emergency event"**

Roles & Responsibilities in the BCP

- Senior Executive Management
  - Consistent support and final approval of plans
  - Setting the business continuity policy
  - Prioritizing critical business functions
  - Allocating sufficient resources and personnel
  - Providing oversight for and approving the BCP
  - Directing and reviewing test results
  - Ensuring maintenance of a current plan
- Senior Functional Management
  - Develop and document maintenance and testing strategy
  - Identify and prioritize mission-critical systems
  - Monitor progress of plan development and execution
  - Ensure periodic tests
  - Create the various teams necessary to execute the plans
- BCP Steering Committee
  - Conduct the **BIA** (**business impact analysis**)
    - **The BIA is all about identifying and prioritizing all business processes based on critically**
  - Coordinate with department representatives
  - Develop analysis group
    - Plan must be developed by those who will carry out
    - Representatives from critical departments
- BCP Teams
  - **Rescue**: responsible for dealing with the immediacy of disaster – employee evacuation, "crashing" the server room, etc.
  - **Recovery**: responsible for getting the alternate facility up and running and restoring the <u>most critical services first</u>
  - **Salvage**: responsible for the return of operations to the original or permanent facility (reconstitution) [<u>least critical services</u>]
- Developing the Teams
  - Management should appoint members
  - Each member must understand the goals of the plan and be familiar with the department they are responsible for
  - Agreed upon prior to the event:

        - Who will talk to the media, customers, share holders
        - Who will setup alternative communication methods
        - Who will setup the offsite facility
        - Established agreements with off-site facilities should be in place
        - Who will work on the primary facility

7 Phases of BCP

1. **Project initiation**
    - Obtain senior management's support
    - Secure funding and resource allocation
    - Name BCP coordinate/project manager
    - Develop project charter
    - Determine scope of the plan
    - Select member of the BCP team
2. **Business impact analysis**
    - Initiated by BCP committee
    - Identifies and prioritizes all business processes
    - Addresses the impact on the organization in the event of loss of a specific services or process
        - **i.** Quantitative: loss of revenue, loss of capital, loss due to liabilities, penalties and fines, etc.
        - **ii.** Qualitative: loss of service quality, competitive advantage, market share, reputation, etc.
    - Establish key metrics for use in determining appropriate counter measures and recovery strategy
    - IMPORTANCE (relevance) vs. CRITICALITY (downtime)
        - **i.** the auditing department is certainly important, though not usually critical. *THE BIA FOCUSES ON CRITICALITY
    - **Key metrics to establish**:
        - **i.** Service level objectives
        - **ii.** RPO (Recovery Point Objective)
        - **iii.** MTD (Maximum Tolerable Downtime)
            1. RTO (Recovery Time Objective)
            2. WRT (Work Recovery Time)
        - **iv.** MTBF (Mean Time Between Failures)
        - **v.** MTTR (Mean Time to Repair)
        - **vi.** MOR (Minimum Operating Requirements)
3. **Recovery strategy**
4. **Plan design and development**
5. **Implementation**
6. **Testing**
7. **Maintenance**

Elements of the Plan: Business Impact Analysis

- Management should establish recovery priorities for business processes that identify:
    - Essential personnel
        - Succession plans
        - MOAs/MOUs (memorandums of agreement/understanding)
    - Technologies
    - Facilities
    - Communications systems
    - Vital records and data

- **Results of the BIA contain:**
    - Identified ALL business processes and assets, not just those considered critical.
    - Impact company can handle dealing with each risk
    - Outage time that would be critical vs those which would not be critical
    - Preventive controls
    - Document and present to management for approval
    - Results are used to create the recovery plans
- **Identify recovery strategies**
    - When preventative controls don't work, recovery strategies are necessary
        - Facility recovery
            - Subscription services
            - Hot, warm, cold sites
            - Reciprocal agreements
            - Offsite facilities should be no less than 15 miles away for low to medium environments. Critical operations should have an office facility 50-200 miles away
            - Reciprocal agreements:
                - How long will the facility be available to the company in need?
                - How much assistance will the staff supply in the means of integrating the two environments and ongoing support?
                - How quickly can the company in need move into the facility?
                - What are the issues pertaining to interoperability?
                - How many of the resources will be available to the company in need?
                - How will differences and conflicts be addressed?
                - How long does change control and configuration management take place?
        - Hardware and software recovery
            - Technology recovery is dependent upon good configuration management documentation
            - Hardware May include
                - PC's/Servers
                - Network equipment
                - Supplies
                - Voice and data communications equipment
                - SLA's can play an essential role in hardware recovery
        - Personnel recovery
            - Identify essential personnel – entire staff is not always necessary to move into recovery operations
            - How to handle personnel if the offsite facility is a great distance away
            - Eliminate single points of failure in staffing and ensure backups are properly trained
            - Don't forget payroll!
            -
        - Data recovery

- Data recovery options are driven by metrics established in the BIA (the MTD, RPO, etc.)
- Backups
- Database shadowing
    - Disk-shadowing
    - Updating one or more copies of data at the same time
    - Data saved to two media types for redundancy
- Electronic vaulting
    - Batch process of moving data
    - Transfer bulk backup information
- Remote journaling
    - Moves the journal or transaction log to a remote location, not the actual files

- **Plan and design development**
    - Now that all the research and planning has been done, this phase is where the actual plan is written
    - Should address:
        - Responsibility
        - Authority
        - Priorities
        - Testing
- **Implementation**
    - Plan is often created for an enterprise with individual functional managers responsible for plans specific to their departments
    - Copies of plan should be kept in multiple locations
    - Both electronic and paper copies should be kept
    - Plan should be distributed to those with a need to know. Most employees will only see a small portion of the plan
    - Three phases following a disruption:
        - Notification/activation
            - Notifying personnel, performing a damage assessment
        - Recovery phase – failover
            - Actions taken by recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities – performed by recovery team
        - Reconstitution – failback
            - Outlines actions taken to return the system to normal operating conditions – performed by salvage team
- **Testing**
    - Should happen once per year, or as the result of a major change (VERY TESTABLE)
    - The purpose of testing is to improve the response (never to find fault or blame)
    - The type of testing is based upon criticality of the organization, resources available and risk tolerance
    - Testing happens before implementation of a plan. The goal is to ensure the accuracy and the effectiveness of the plan. Have a 3rd party auditor monitor how the plans are carried out.
    - Types of tests:
        - Checklist test
            - Copies of plan distributed to different departments

            - Functional managers review
        - Structured walk-through (table top) test
            - Representatives from each department go over the plan
        - Simulation test
            - Going through a disaster scenario
            - Continues up to the actual relocation to an offsite facility
        - Parallel test
            - Systems moved to alternate site, and processing takes place there
        - Full-interruption test
            - Original site shut down
            - All of processing moved to offsite facility
    - Post incident review; after a test or disaster has taken place:
        - Focus on what happened
        - What should have happened
        - What should happen next
        - Not whose fault it was; this is not productive!
- **Maintenance**
    - Change management:
        - Technical – hardware/software
        - People**,** Environment**,** Laws
    - Large plans can take a lot of work to maintain
    - Does not have a direct line to profitability
    - Keeping plan in date
        - Make it a part of business meetings and decisions
        - Centralize responsibility for updates
        - Part of job description
        - Personnel evaluations
        - Report regularly
        - Audits
        - As plans get revised, original copies should be retrieved and destroyed

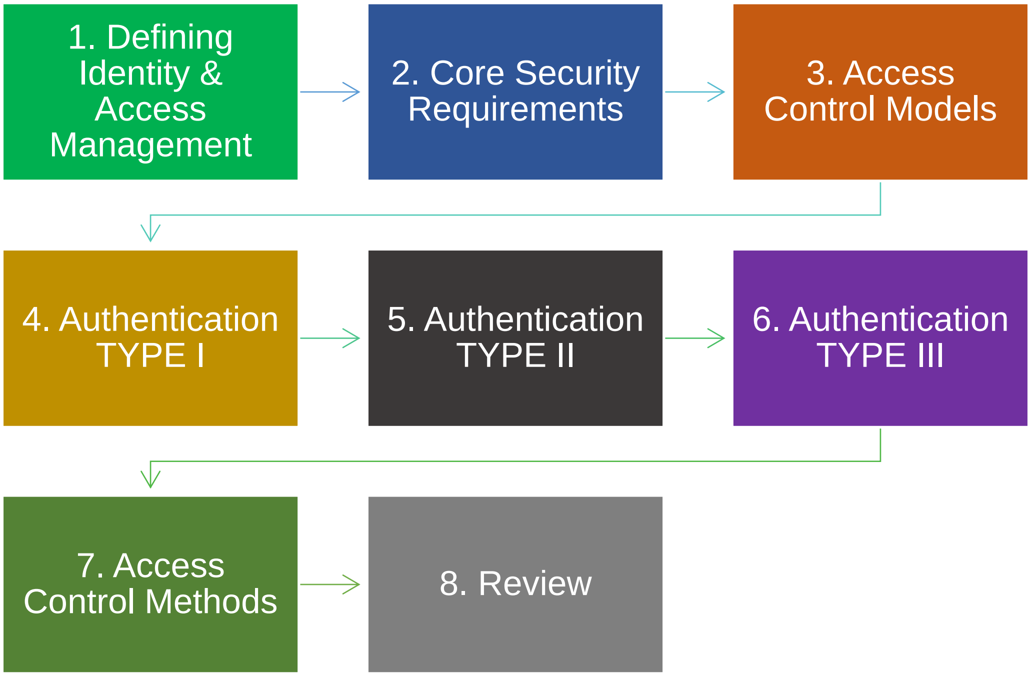
5. Risk Monitoring & Reporting

Intrusion Detection Systems

- Software is used to monitor a network segment or an individual computer
- Used to detect attacks and other malicious activity
- Dynamic in nature
- The two main types:
    - Network-based
    - Host-based systems (TCP Wrappers)
- Type of IDS:
    - Network-based ISD
        - Monitors traffic on a network segment
        - Computer or network appliance with NIC in promiscuous mode
        - Sensors communicate with a central management console
    - Host-based IDS
        - Small agent programs that reside on individual computer
        - Detects suspicious activity on one system, not a network segment
    - IDS components:
        - Sensors

        - Analysis engine
        - Management console
- Senor placement:
    - In front of firewalls to discover attacks being launched
    - Behind firewalls to find out about intruders who have gotten through
    - On the internal network to detect internal attacks
    - A good place to put sensors is in the DMZ
- Analysis engine methods:
    - Pattern matching
        - Rule-based intrusion detection
        - Signature-based intrusion detection
        - Knowledge-based intrusion detection
    - Profile comparison
        - Statistical-based intrusion detection
        - Anomaly-based intrusion detection
        - Behavior-based intrusion detection
- Types of IDS
    - Signature based – most common
        - IDS has a database of signatures, which are patterns of previously identified attacks. Cannot identify new attacks. Database needs continual updates.
    - Behavior-based
        - Compares audit files, logs, and network behavior, and develops and maintains profiles of normal behavior. Better defense against new attacks. Creates many false positives.
    - Today, we should be using a combination of both,
- IDS response options
    - Passive:
        - Page or e-email admins; log events
    - Active:
        - Send reset packets to the attacker’s connections
        - Change a firewall or router ACL to block an IP address or range
        - Reconfigure router or firewall to block protocol being used for attack
- IDS Issues
    - May not be able to process all packets on large networks
        - Missed packets may contain actual attacks
        - IDS vendors are moving more and more to hardware-based systems
    - Cannot analyze encrypted data
    - Switch-based networks make it harder to pick up all packets
    - A lot of false alarms
    - Not an answer to all prayers
        - Firewalls, anti-virus software, policies, and other security controls are important
- Utilize for continuous monitoring:
    - IDS/IPS monitoring
    - Vulnerability assessments
    - Penetration testing

III. ACCESS CONTROL & IDENTITY MANAGEMENT:


1. Defining Identity & Access Management
2. Core Security Requirements
3. Access Control Models
4. Authentication TYPE I
5. Authentication TYPE II
6. Authentication TYPE III
7. Access Control Methods
8. Review

1. Defining Identity & Access Management

- Authentication and Identity Management
  - Identification: making a claim
  - Authentication allows users to support the claim of their identity
  - Identity and access management
    - Services/policies/procedures for managing a digital identity/provisioning
  - Security controls (including management) are audited annually under Sarbanes-Oxley (SOX)

Credential Management

- Exploits
  - MITM & traffic hijacking
  - Unauthorized access
  - Privilege escalation
- Solutions
  - Certificates
  - Single sign on

2. Core Security Requirements

Authenticity (example requirements)

- Users must provide authentication information at login, but shall not have to provide this information for subsequent access to intranet resources
- For access to financially sensitive information, subjects shall be required to authenticate via a smart card and a PIN
- Internal and External users should be able to access the software
- Mutual authentication will be supported through the use of certificates

Authorization

- Confirms that an authenticated entity has the privileges and permissions necessary

- CRUS operations - (Create, Read, Update, Delete)
- Access control models:
  - DAB: discretionary access control
  - MAC: mandatory access control
  - RBAC: role based access control
  - RuBAC: rule based access control (typically on firewalls)
- Example requirements:
  - Access to highly sensitive information will be restricted to users with Secret or Top Secret clearance
  - Unauthenticated users will only have read permission to public access pages
  - Only those with administrative credentials will be able to modify files

Accountability

- Tracing an action to a subject – also known as auditing
- Must include the following:
  - Identity of subject
  - The action
  - Object on which the action was performed
  - Timestamp
- Examples requirements:
  - All failed logon attempts will be logged with timestamp and source IP address
  - Audit logs should not overwrite previous events. They should append to previous entry and alert admin when space becomes limited
  - Audit logs must be retained for one year

3. Access Control Models

DAC

- Discretionary Access Control
  - Security of an object is at the owner's discretion
  - Access is granted through an ACL (access control list)
  - Commonly implemented in commercial products and all client based systems
  - Identity based
  - Almost all client, and many servers based systems use DAC for its ease of use and sharing capabilities

MAC

- Mandatory Access Control
  - Data owners cannot grant access
  - OS makes the decision based on a security label system
  - Subject's label must dominate the object's label
  - Users and data are given a clearance level (confidential, secret, top secret, etc.)
  - Rules for access are configured by the security officer and enforced by the OS
  - MAC systems are for very secure environments and rely on labels

RBAC

- Role Based Access Control
  - Based on role of user within the organization, good for preventing authorization creep.
  - RBAC is sometimes referred to as Non-Discretionary Access Control because the owner of an object does not control access. Each role as a set of rights and permissions which cannot be changed (without security admin's involvement.)

4. Authentication TYPE I

Proving your identity

- Type 1: something you know
- Type 2: something you have
- Type 3: something you are

Type 1:

- Passwords/passphrases/cognitive password/PINs
- Best practices
  - No less than 8 characters
  - Change on a regular basis
  - Enforce password history
  - Consider brute force and dictionary attacks
  - Ease of cracking cognitive passwords
  - Graphic image
  - Enable clipping levels and respond accordingly

5. Authentication TYPE II

Something you have

- Token devices
- Smart card
- Memory card
- Hardware key
- Cryptographic key
- Certificate
- Cookies

Token devices: one time password generators

- One time password reduces vulnerability associated with sniffing passwords
- Simple device to implements
- Can be costly
- Users can lose or damage
- Two types: synchronous/asynchronous

Synchronous token devices

- Rely upon synchronizing with authentication server
- Frequently time based, but could be event based
- If damaged, or battery files, must be-resynchronized
- Authentication server knows what “password’ to expect based on time or event

Asynchronous token devices

- Aka challenge response
- User logs in
- Authentication returns a challenge to the user
- User types challenge string into token device and presses enter
- Token devices returns a reply
- Only that specific users token device could respond with the expected reply
- More complex than synchronous
- May provide better protection against sniffing

Memory cards

- Holds information, does not process
- A memory card holds authentication info, <u>usually you’ll want to pair this with a PIN</u>

- A credit card or ATM card is a type of memory, so is a key/swipe card
- Usually insecure, easily copied*

Smart card (191)

- More secure than memory cards
- Can process information
- Includes a microprocessor
- Often integrated with PKI
- Two types:
    - Contact
    - Contactless
- ATTACKS
    - There are attacks against smart cards
    - Fault generation – manipulative environmental controls and measure errors to reverse engineer logic
    - Side channel attacks – measure the cards while they work
        - Differential power analysis – measure power emissions
        - Electromagnetic analysis – example frequencies emitted
    - Micro probing – using needles to vibrations to remove the outer protection on the cards circuits. Then tap into ROMS if possible or "die" ROMS to read data.

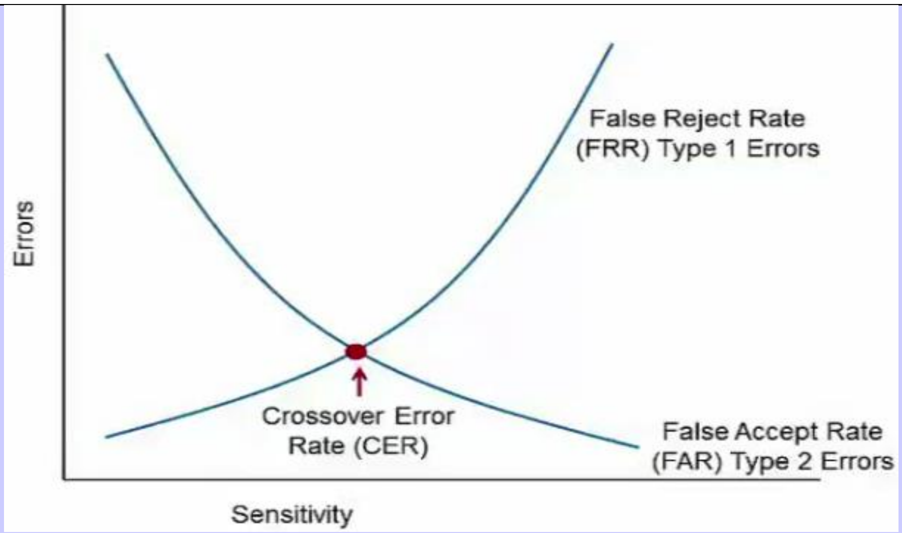
6. Authentication TYPE III

Something you are

- Biometrics
    - **Static**: should not significantly change over time. Bound to a user's physiological traits: fingerprint, hand geometry, iris, retina, etc.
    - **Dynamic**: based on behavioral traits
        - Voice, gait, signature, keyboard cadence, etc.
        - Even though these can be modified temporarily, they are very difficult to modify for any significant length of time

Biometric concerns

- Accuracy
    - **Type I error**: false rejection – a legitimate user is barred from access. Is caused when a system identities too much information. This causes excessive overhead.
    - **Type II error**: false acceptance – an imposter is allowed access. This is a security threat and comes when a system doesn't evaluate enough information
    - As **FRR** goes down, **FAR** goes up and vice versa
    - The level at which the two meet is called the **CER** (crossover errors rate). The lower the number, the more accurate the system
    - Iris scans are the most accurate

- ○ 

- User acceptance
- Many users feel biometrics are intrusive
  - Retina scans can reveal health care information
- Time for enrollment and verification can make user's resistant
- Cost/benefit analysis
- No way to revoke biometrics
- Cost
- Biometric systems can be very costly and require unwieldy technology
- Though costs are coming down for means like fingerprint recognition, other technologies remain prohibitive

The best authentication is the combination of 2 or more than one type, multifactor

7. Access Control Methods

Rule based access control

- Uses specific rules that indicate what can and cannot transpire between subject and object.
- Also, called non-discretionary
- "if x then y" logic
- Before a subject can access an object, it must meet a set of predefined rules
  - Ex. If a user has proper clearance, and it's between 9am – 5pm then allow access (context based access control)
- However, it does NOT have to deal specifically with identify/authorization
  - Ex. May only accept email attachments 5Mb or less
- Is considered "compulsory control" because the rules are strictly enforced and not modified by users.
- Routers and firewalls use rule based access control

Constrained user interfaces

- Restrict user access by not allowing them to see certain data or have certain functionality
- Views – only allow access to certain data (canned interfaces)
- Restricted shell – like a real shell but only with certain commands (like Cisco's non-enable mode)

- Menu – similar but more “GUI”
- Physically constrained interface – show only certain keys on a keypad/touch screen. Like an ATM. (a modern type of menu) Difference is you are physically constrained from accessing them.
    -

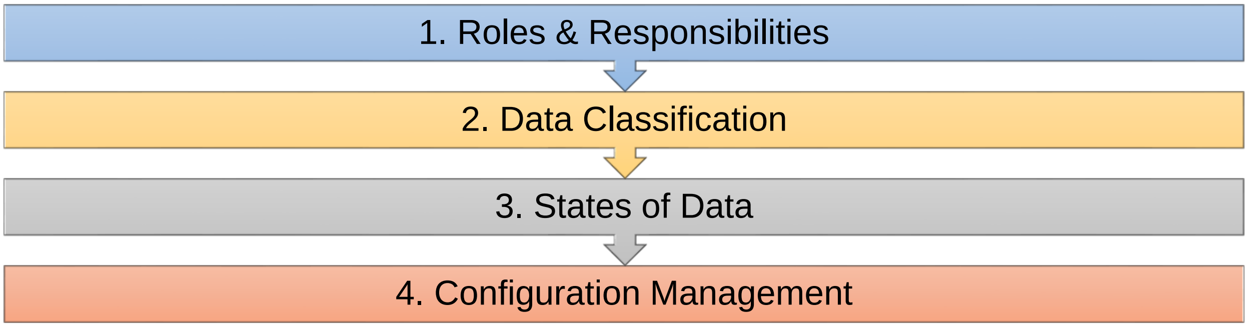
Content & context dependent access controls

- Content
    - Access is determined by the type of data.
    - Ex. Email filters that look for specific things like “confidential”, “SSN”, images.
    - Web proxy servers may be content based
- Context
    - System reviews a situation then makes a decision on access
    - a firewall is a great example of this, if session is established, then allow traffic to proceed
    - in a web proxy, allow access to certain body imagery if previous web sessions are referencing medical data otherwise deny access.

8. Identify & Access Management Review

- IAAA (identification, authentication, authorization, accounting)
    - Identification
    - Authentication
        - Type I (something you know)
        - Type II (something you have)
        - Type III (biometrics)
    - Single sign on (Kerberos)
- Access control models
- Access control methods
- Access control administration (RADIUS)
- Data emanation

IV. ASSET SECURITY FRAMEWORK



1. Roles & Responsibilities

- Senior/Executive Management
  - **CEO**: Chief Decision-Maker
  - **CFO**: Responsible for budgeting and finance
  - **CIO**: Ensures technology supports company's objectives
  - **ISO**: Risk Analysis and Mitigation
- **Steering Committee**: Defines risk, objectives and approaches
- **Auditors**: evaluates business processes
- **Data owner**: classifies data
- **Data custodian**: day to day maintenance of data
- **Network administrator**: ensures availability of network resources
- **Security administrator**: responsible for all security-related tasks, focusing on Confidentiality and Integrity.

Responsibilities of the ISO:

- Responsible for providing C-I-A for all information assets
- Communication of Risks to senior management
- Recommend best practices to influence policies, standards, procedures, guidelines
- Establish security measurements
- Ensure compliance with government and industry regulations
- Maintain awareness of emerging threats

2. Data Classification

- Development of sensitivity labels for data and the assignment of those labels for configuring baseline security based on value of data
- **Cost**: value of the data
- **Classify**: criteria for classification
- **Controls**: determining the baseline security configuration for each
- Data owner determines the classification of data
- Data custodian maintains the data

Considerations for Asset Valuation

- What makes up the value of an asset?
- Value to the organization
- Loss if compromised
- Legislative drivers
- Liabilities
- Value to competitors

- Acquisition costs
- And many others

Sensitivity vs. Criticality

- **Sensitivity** describes the amount of damage that would be done should the information be disclosed
- **Criticality** describes the time sensitivity of the data. This is usually driven by the understanding of how much revenue a specific asset generates, and without that asset, there will be lost revenue.

3. States of Data

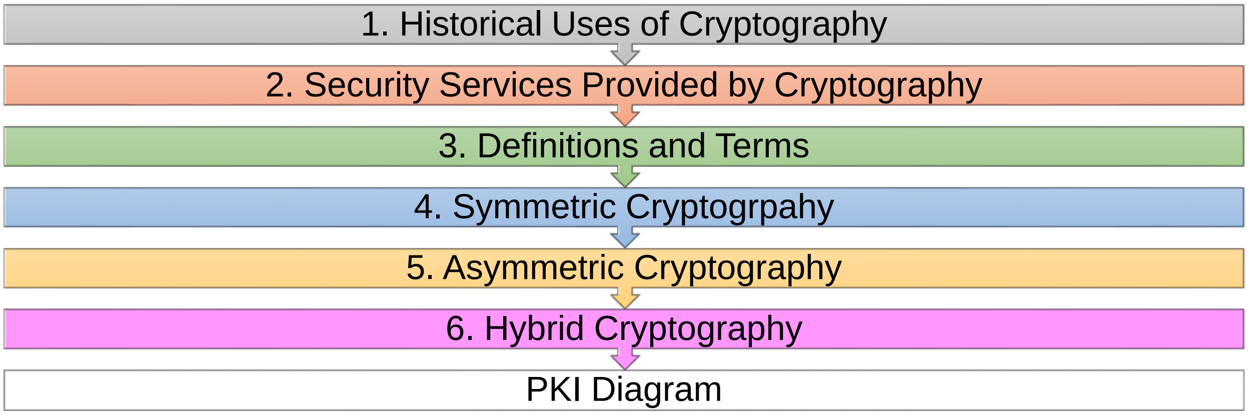
- **At rest**: File system encryptions, EFS (encrypted file system [Windows]), TPM (trusted platform module, allows whole drive encryption)
- **In Process**: Use proper controls
- **In Transit**: Use secure transit protocols; IPSec, SSL/TLS

4. Configuration Management

- System hardening & baselining
  - Removing necessary services
  - Installing the latest service packs and patches
  - Renaming default accounts
  - Changing default setting
  - Enabling security configurations like auditing, firewalls, updates, etc.
  - *Don't forget physical security!
- Config Mgmt.:
  - Defined by ISC2 as "a process of identifying and documenting hardware components, software and the associated setting."
  - The goal is to move beyond the original design to a hardened, operationally sound configuration
  - Identifying, controlling, accounting for and auditing changes made to the baseline TCB
  - These changes come about as we perform system hardening tasks to secure a system
  - Will control changes and test documentation through the operational life cycle of a system
  - Implemented hand in hand with change control
  - ESSENTIAL to disaster recovery
- Configuration mgmt. documentation:
  - Make
  - Model
  - MAC address
  - Serial number
  - Operating system/firmware version
  - Location
  - BIOS or other passwords
  - Permanent IP if applicable
  - Organizational department label
- Change Management:

- Directive, administrative control that should be incorporated into organizational policy.
- The formal review of all proposed changes – NO “on-the-fly” changes!

V. CRYPTOGRAPHY FRAMEWORK:



1. Historical Uses of Cryptography
2. Security Services Provided by Cryptography
3. Definitions and Terms
4. Symmetric Cryptogrpahy
5. Asymmetric Cryptography
6. Hybrid Cryptography

PKI Diagram

6. Historical Uses of Cryptography

- **Caesar Cipher**
  - Simple substitution
  - Shift characters 3 spaces
  - A=D, B=E, C=F, etc.
  - Substitution Ciphers are subject to pattern analysis
- **Scytale Cipher**
  - Spartans used this cipher to communicate messages to generals in the field
  - Wrapped tape around a rod
  - Diameter of the rod is the pre-agreed upon secret (key)
- **Vignere Cipher**
  - First polygraphic cipher
  - Key word is agreed upon ahead of time
  - First letter of the key is matched up against first letter of the message, and so on
- **Cryptography in warfare**
  - Enigma machine/purple machine
  - Used by the Germans/Japanese in WWII
  - Breaking the cryptography of these devices is credited with reducing the length of the war.
- **Vernam cipher**
  - One Time Pad
  - Only mathematically unbreakable form of cryptography
    - Key must be used only once
    - Pad must be at least as long as the message
    - Kay pad is statistically unpredictable
    - Key pad must be delivered and stored securely

7. Security Services Provided by Cryptography

- **Privacy**: prevents unauthorized disclosure of information
- **Authenticity**: verifies the claimed identity
- **Integrity**: detects modification or corruption
- **Non-repudiation**: combines authenticity and integrity. A sender can't dispute having sent a message, nor its contents.

8. Definitions & Terms

- **Conceptual crypto formula:**
  - Plain text + Initialization Vector + Algorithm (aka Cipher) + Key = Cipher Text

Initialization Vector (Adding randomness to the start)

- Here are some random numbers: 7 5 2 3 4 9 4
  - If we start at track 0 and +7 +5 -2 +3 +4 +9 -4
  - We still don't have randomness. Vary the starting point and that will make the process more random.
- Very similar to a "seed" or a "salt"

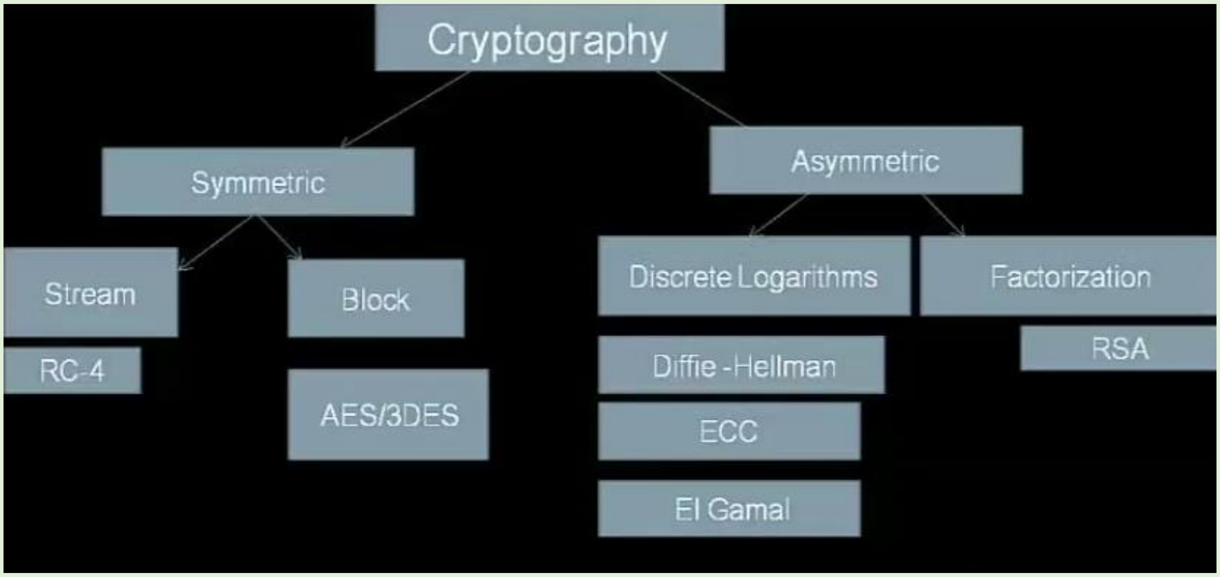
Algorithm

- Collection of all math functions that can be performed
- Desirable qualities of algorithm
  - Confusion: the strength of the math drives the complexity of the substitution
  - Diffusion: allows for the use of the plain text in the ciphertext
  - Avalanche
  - Permutations
  - Open – Kirchhoff's principle

Key

- Desirable qualities of a key
  - Long
  - Random
  - Secret

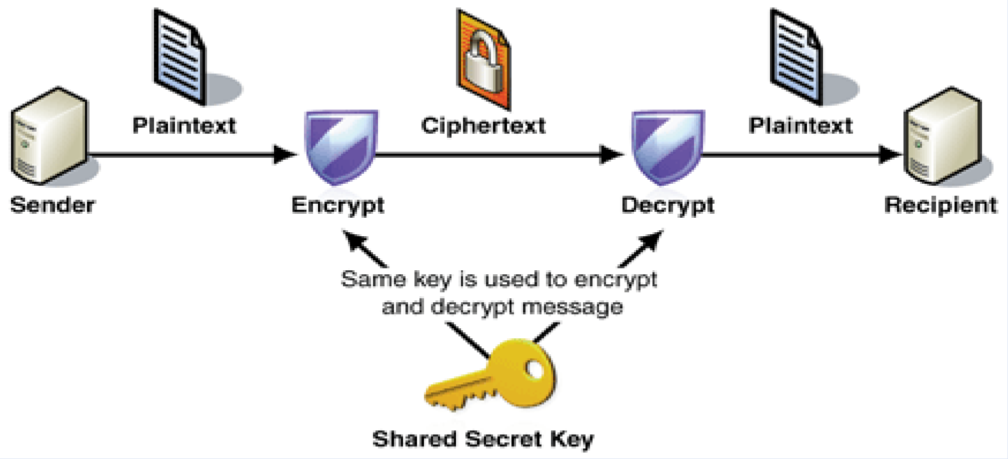
Breakdown:



9. Symmetric Cryptography

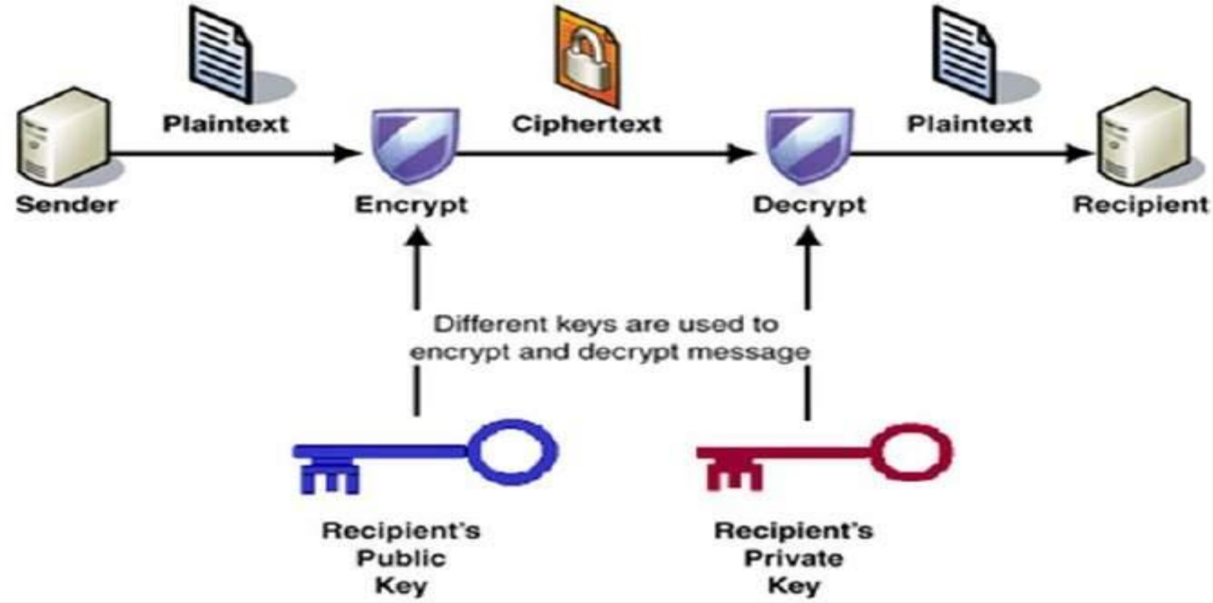
1. Symmetric = same

2. In symmetric cryptography, the same key is used to both encrypt and decrypt
3. Very fast means of encrypting/decrypting with good strength for privacy
4. Proffered means of protecting privacy data
5. Also, can be called “Private Key” “Secret Key” or “Shared Key”
6. Drawbacks to symmetric cryptography
   - Out of band key exchange
   - Not scalable
   - No authenticity, integrity, or non-repudiation



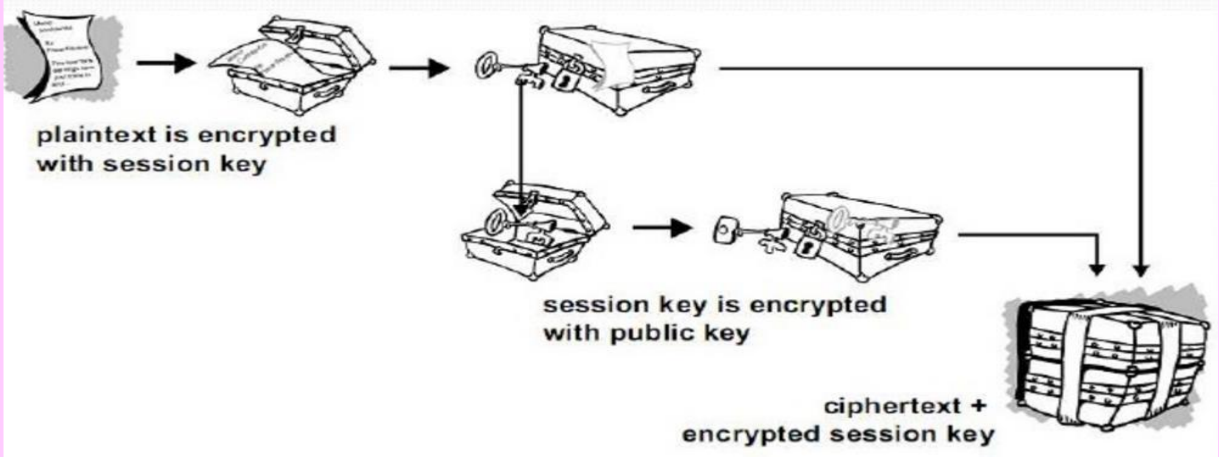
10. Asymmetric Cryptography

1. Every user has a key pair
   - Public key is made available to anyone who requests it
   - Private key is only available to that user and must not be disclosed or shared
2. The keys are mathematically related so that anything is encrypted with one key can only be decrypted by the other

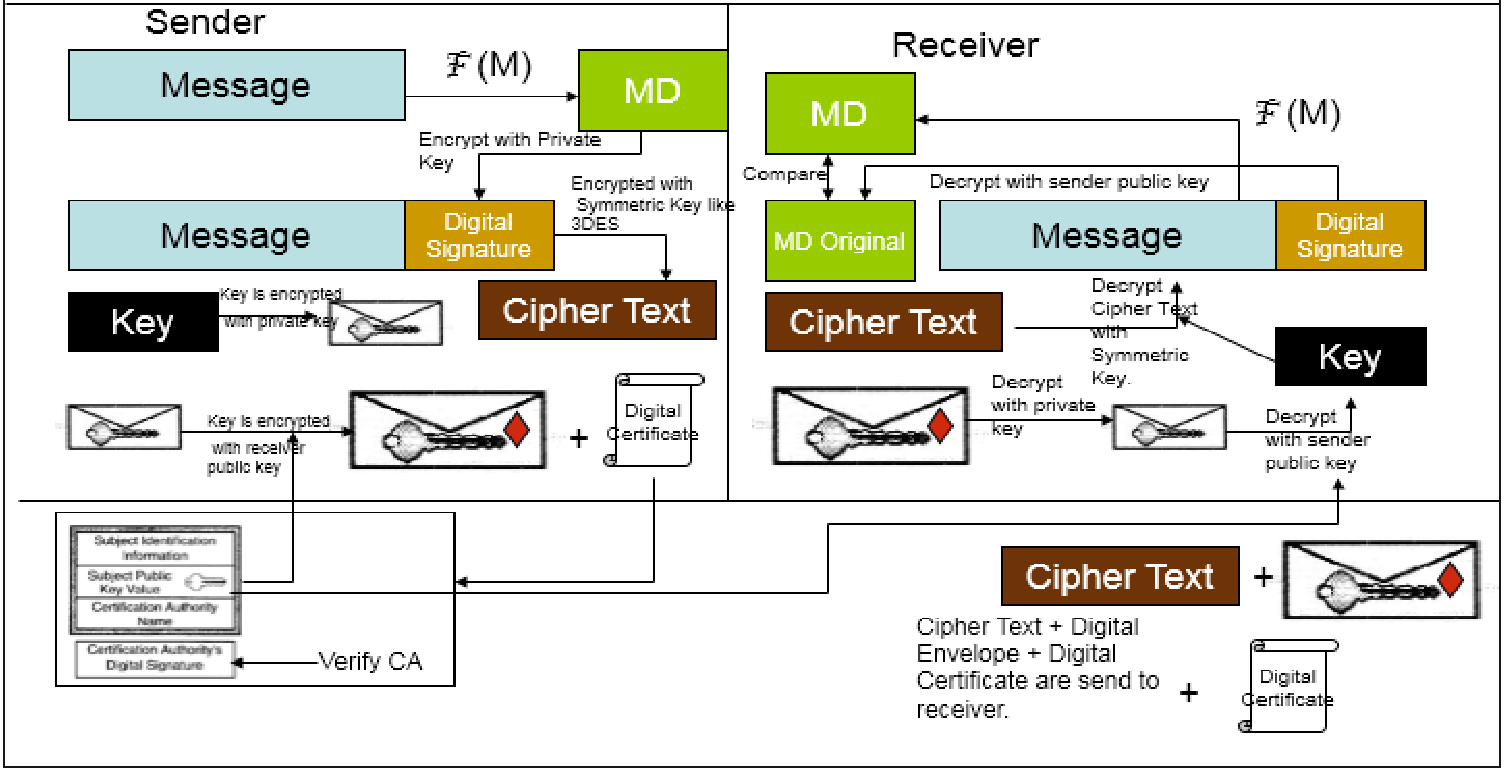


11. Hybrid Cryptography

1. Client initiates a secure connection
2. Server responds by sending its public key to the client
3. The client then generates a symmetric session key
4. Client encrypts uses the server's public key to encrypt the session key
5. Client sends the session key (encrypted with the server's public key) to the server
6. Server uses its private key to decrypt the session
7. Now that a symmetric session key has been distributed, both parties have a secure channel in which to communicate.


plaintext is encrypted with session key
session key is encrypted with public key
ciphertext + encrypted session key

How does PKI Work?



Sender

Message

𝓕 (M)

MD

Encrypt with Private Key

Message

Digital Signature

Encrypted with Symmetric Key like 3DES

Cipher Text

Key

Key is encrypted with private key

Key is encrypted with receiver public key

+

Digital Certificate

Subject Identification Information

Subject Public Key Value

Certification Authority Name

Certification Authority's Digital Signature

Verify CA

Receiver

MD

𝓕 (M)

Compare

Decrypt with sender public key

MD Original

Message

Digital Signature

Cipher Text

Decrypt Cipher Text with Symmetric Key.

Key

Decrypt with private key

Decrypt with sender public key

Cipher Text

+

Cipher Text + Digital Envelope + Digital Certificate are send to receiver.

+

Digital Certificate