ISC2 Code of Ethics:

Code of Ethics Preamble:

Safety of the commonwealth, duty to our principals (employers, contractors, people we work for), and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- **Protect society, the commonwealth, and the infrastructure**
  - Promote and preserve public trust and confidence in information and systems
  - Protect society, the commonwealth, and the infrastructure
  - Promote and preserve public trust and confidence in information and systems
  - Promote the understanding and acceptance of prudent information security measures
  - Preserve and strengthen the integrity of the public infrastructure
  - Discourage unsafe practice
- **Act honorably, honestly, justly, responsibly, and legally**
  - Tell the truth; make all stakeholders aware of your actions on a timely basis
  - Observe all contracts and agreements, express or implied
  - Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order
  - Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence
  - When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service
- **Provide diligent and competent service to principals**
  - Preserve the value of their systems, applications, and information
  - Respect their trust and the privileges that they grant you
  - Avoid conflicts of interest or the appearance thereof
  - Render only those services for which you are fully competent and qualified
- **Advance and protect the profession**
  - Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
  - Take care not to injure the reputation of other professionals through malice or indifference
  - Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others

Objectives for Guidance:

- **Give Guidance for resolving good versus good, and bad versus bad, dilemmas**
- **To encourage right behavior such as:**
  - Research
  - Teaching
  - Finding & Mentoring valuable candidates for the certification
  - Valuing the certificate
- **To discourage behavior such as:**
  - Raising unnecessary alarm, fear, uncertainty, or doubt
  - Consenting to bad practice
  - Attaching weak systems to the public network
  - Associating or appearing to associate with criminals or criminal behavior
  - Professional association with non-professionals
  - Professional recognition of or association with amateurs

Risk Management:

Terms & Definitions:
Asset: Valuable resources you're trying to protect (people, data, systems, buildings, etc.)
Vulnerability: A weakness is a system that allows a threat to cause harm | A gap in protection
Threat: A potentially harmful occurrence (DoS attack, virus, tornado, power outage, etc.)
Threat Agent: An entity acting against an asset
Threat Vector: The medium through which a threat agent exploits a vulnerability (ex. email attachment, open port)
Impact: The severity of the damage, usually expressed in dollars
Exposure: An instance of being exposed to losses from a threat agent exploiting a vulnerability
Risk: The likelihood of a threat agent leveraging an asset to act against an asset (Requires a loss)
The probability of damage occurring and the ramifications of the potential damage
Risk= Threat x Vulnerability | Risk= Threat x Vulnerability x Cost | Risk= Threat x Vulnerability x Impact
Any risk involving the loss of human life is extremely high and must be mitigated
Threat Agents give rise to *Threats* which *Exploit Vulnerabilities* which leads to *Risk* which damage *Assets*
Safeguard: A measure taken to reduce risk
(TCO) Total Cost of Ownership: The cost of a safeguard (up-front cost + annual cost of maintenance)
(ROI) Return on Investment: Money saved by deploying a safeguard (safeguards shouldn't cost more than asset)
Risk Analysis: Identify assets, discover threats that put them at risk, and estimate potential loss
Risk Decisions: Determine which safeguards we deploy to protect our assets, and the budget for doing so
Security Governance: The organizational structure required for a successful information security program
People: Most valuable asset. Any risk involving loss of human life is Extremely high and must be mitigated
Infosec: A management issue that may require technical solutions

Calculating Loss Expectancy:
(AV) Asset Value: The value of the asset you're trying to protect
(EF) Exposure Factor: Percentage of value an asset lost due to an incident (2 story home, flooded 1st floor= 50%)
(SLE) Single Loss Expectancy: The cost of a single loss **(SLE= AV x EF)**
(ARO) Annual Rate of Occurrence: The number of losses suffered per year (or estimated # of losses per year)
(ALE) Annualized Loss Expectancy: Annual cost due to risk **(ALE= SLE x ARO)**
(TCO) Total Cost of Ownership: The total cost of a mitigating safeguard (up-front cost + annual maint. cost). Includes staff hours, vendor maintenance fees, subscription fees, and other operational costs for **1 year**.
(ROI) Return on Investment: Amount of money saved by implementing a safeguard. If your annual TCO is less than your ALE, you have a positive ROI (good choice).

Table 2.3 Annualized Loss Expectancy of Unencrypted Laptops

	Formula	Value
Asset value (AV)	AV	$25,000
Exposure factor (EF)	EF	100%
Single loss expectancy (SLE)	AV × EF	$25,000
Annual rate of occurrence (ARO)	ARO	11
Annualized loss expectancy (ALE)	SLE × ARO	$275,000

Table 2.4 Annualized Loss Expectancy of Encrypted Laptops

	Formula	Value
Asset value (AV)	AV	$25,000
Exposure factor (EF)	EF	10%
Single loss expectancy (SLE)	AV × EF	$2500
Annual rate of occurrence (ARO)	ARO	11
Annualized loss expectancy (ALE)	SLE × ARO	$27,500

TCO of laptop encryption= $136,667/year
Annual Savings for encryption= $247,500 (Old ALE – new ALE)
ROI= $110,883/year ($247,500 – $136,667)

Information Risk Management:

- The process of identifying risk, assessing risk, reducing risk to an acceptable level, & maintaining that level
- **Mission**: To evaluate risks against our critical assets, and deploy safeguards to mitigate those risks
- **Goals**:
  - Identify assets and their value
  - Identify vulnerabilities and threats to the asset
  - Quantify probability and business impact of potential threats (Risk)
  - Determine needs
  - Deploy a positive ROI safeguard
  - Monitor and evaluate systems & practices
  - Promote security awareness
- **Requirements:** Sr. Mgmt. support, documented processes that support the business mission
  - Senior Management support
  - Documented processes that support the business mission
  - An Information Risk Management policy (a subset of the organization's overall risk mgmt. policy)
  - A dedicated IRM team
- **Risk Management Process (NIST 800-30):**
  1. System Characterization: describes scope of risk management effort & systems to be analyzed
  2. Threat Identification
  3. Vulnerability Identification
  4. Control Analysis
  5. Likelihood Determination
  6. Impact Analysis
  7. Risk Determination
  8. Control Recommendations
  9. Results Documentation
- **Risk Categories:**
  1. Physical damage
  2. Human interaction
  3. Equipment malfunction
  4. Misuse of data
  5. Inside & outside attacks
  6. Loss of data
  7. Application error

(CIA) Information Security Triad:

Goal: To balance the needs of the three, making trade-offs when necessary

- **Confidentiality**: Prevents unauthorized read access to data (prevents unauthorized disclosure of info)
- **Integrity**: Prevents unauthorized write access to data (prevents unauthorized modification of info)
- **Availability**: Ensures information is available when needed

(AAA) Identity and Authentication, Authorization, and Accountabilty:

- **Identity**: An identity claim is someone stating who they are (ex. User Name) [NO Proof]
- **Authentication**: Proving an identity claim by supplying secret information (ex. Password)
- **Authorization**: The actions permitted once Identification & Authorization take place (Permissions)
- **Accountability**: Holds users accountable for their actions, typically through logging & monitoring

Other Key Security Concepts:

- **Nonrepudiation:** User cannot deny having performed a transaction. Authenticates identity of a user who performs a transaction & ensures the integrity of that transaction. Requires Authentication & Integrity.

- **Least Privilege:** User should be granted minimum amount of access (authorization) required to do their jobs, and no more.
- **Need to Know:** More granular than least privilege, and one step farther. The user must have a need to know a specific piece of information before being granted access to it.
- **Defense in Depth:** Layered Defense. Applying multiple controls (safeguards) to reduce risk. Any one security control may fail, so applying multiple increases the CIA of data.

Access Control Categories:

- **Administrative:** Developing & publishing policies, standards, procedures (Ex. Risk Mgmt, Chg. Ctrl)
- **Technical (Logical):** Implementing access control mechanisms, password mgmt, Ident & Auth, etc.
- **Physical:** Controlling individual physical access (Ex. locks, environmental controls, disable USB)

Planning Horizon:

- **Operational:** Short-term plans. Specific tasks with hard deadlines
- **Tactical:** Mid-term plans that deal with initiatives that support the Strategic Plan
- **Strategic:** Follow long-term (3-5 years) business and technical goals

Risk Analysis:

Risk decisions dictate which safeguards we deploy to protect our assets, and the amount of money spent.

- **Risk:** The likelihood of a threat agent leveraging an asset to act against an asset (Requires a loss). Also, The probability of damage occurring and the ramifications of the potential damage
- **Human Life**: Any risk involving the loss of human life is extremely high and must be mitigated
- **Risk Equations:**
  - Risk= Threat x Vulnerability
  - Risk= Threat x Vulnerability x Cost
  - Risk= Threat x Vulnerability x Impact
- **Risk Choices:**
  - **Accept:** Typically low likelihood/low consequence risks may be accepted
  - **Mitigate/Reduce/Eliminate:** Lowering risk to acceptable level through deploying safeguards
  - **Transfer:** Purchasing an insurance policy protecting you from the risk
  - **Avoid:** Choosing not to do a new project because of the associated risk. Decision based on calculation (Avoid if ALE of new project after mitigation is greater than the ROI of the project)
- **Risk Analysis Methods:**
  - **Qualitative:** Uses simple approximations (low, medium, high, 1-5, 1-10, etc.) for inputs
  - **Quantitative:** Uses hard calculations & metrics (ex. dollars) for inputs
- **Risk Analysis Teams:** Include people from most or all departments to ensure threats are identified
- **Risk Analysis Matrix: Qualitative.** Uses a quadrant to map the likelihood of a risk occurring against the potential impact of it occurring. Used to perform Qualitative Risk Analysis
  - **Matrix Values:**
    - **Low:** Handled via normal process
    - **Med:** Require management notification
    - **High:** Require senior management notification
    - **Extreme:** Require immediate action, detailed mitigation plan, and senior management notification.

Risk Analysis Matrix		Consequences				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5. Almost Certain	H	H	E	E	E
	4. Likely	M	H	H	E	E
	3. Possible	L	M	H	E	E
	2. Unlikely	L	L	M	H	E
	1. Rare	L	L	M	H	H

Information Security Governance: Information security at the organizational level (mgmt, policies, processes…)

- **Laws & Regulations:** (Mandatory) High-level government directives
- **Policy: (**Mandatory) (NIST 800-12) High-level management directives
  - **Types:** Program Policy, Issue-Specific Policy, System-Specific Policy
  - **Contents:** Purpose, Scope, Responsibilities, and Compliance
- **Procedures:** (Mandatory) Step-by-step guide for accomplishing a task
- **Standards:** (Mandatory) Describe the specific use of a technology (ex. laptop make/model/specs)
- **Guidelines:** (Discretionary) Recommendations
- **Baselines:** (Discretionary) Uniform way of doing something. Defines the lowest acceptable security level

Document	Example	Mandatory or Discretionary?
Policy	*Protect the CIA of PII by hardening the operating system*	Mandatory
Procedure	*Step 1: Install pre-hardened OS Image. Step 2: Download patches from update server. Step 3: …*	Mandatory
Standard	*Use Nexus-6 laptop hardware*	Mandatory
Guideline	*Patch installation may be automated via the use of an installer script*	Discretionary
Baselines	*Use the CISecurity Windows Hardening benchmark*	Discretionary

Information Security Roles & Responsibilities:

- **Senior Management:** Creates information security program & ensures staffing, funding & support
  - **Security Officer:** Monitors security program & ensures security directives are fulfilled
  - **Data Owner (Information Owner/Business Owner):** Management employees who determine data classification level & backup frequency. Capital "O"
- **Data Custodian:** Provide hands-on protection of assets. Perform backups, patching, configuration, etc.
- **User:** Comply with mandatory policies, procedures, standards, etc. Require security awareness

Compliance with Laws & Regulations:

- **Privacy:** The protection of the confidentiality of personal information
- **Due Care:** Doing what a reasonable person would do "Prudent Man" rule. Used to determine liability.
- **Due Diligence:** The management of Due Care. Follows a formal process to verify Due Care is occurring
- **Gross Negligence:** The opposite of Due Care. If you cannot demonstrate due care, you are likely this
- **Best Practice:** A consensus of the best way to protect the CIA of assets. Used to demonstrate Due Care

Security Frameworks:

Auditing: Verifying compliance to a security control framework (or published specification)
Describes What is to Achieve: COBIT and COSO
Describes How to Achieve it: ITIL & ISO 27000 series

- **(OCTAVE) Operationally Critical Threat, Asset, and Vulnerability Evaluation:**
  - Three phase Risk Management framework
    - Phase 1: Identify staff knowledge, assets, and threats
    - Phase 2: Identify vulnerabilities and evaluate safeguards
    - Phase 3: Conduct risk analysis and develop risk mitigation strategy
- **(COBIT) Control Objectives for Information and Related Technology:**
  - Operational framework & best practices Model for IT Governance
  - Defines goals for controls that should be used to manage IT and ensure IT maps to business needs
  - 4 Domains (34 Processes):
    - Plan & Organize
    - Acquire & Implement
    - Deliver & Support
    - Monitor & Evaluate

- **(COSO) Committee of Sponsoring Organizations**
  - Strategic Model for Corporate Governance
  - 5 Components:
    - Control Environment
    - Risk Assessment
    - Control Activities
    - Communication of Information
    - Monitoring
- **(ITIL) Information Technology Infrastructure Library)**
  - Customizable framework for providing best services in IT Service Management (ITSM)
  - 5 Service Management Practices-Core Guidance publications
    - Service Strategy (helps IT provide services)
    - Service Design (designing infrastructure & architecture)
    - Service Transition (making projects operational)
    - Service Operation (operations controls)
    - Continual Service Improvement (ways to improve existing services)

Information Security Standards:

- **Risk Assessment:** NIST 800-30 | NIST 800-66
- **BS 17799:** Old British standard
  - **Part 1:** Control Objectives
  - **Part 2:** Establishing & Maintaining a security program
- **ISO 27000 Series:**
  - **27001:** Establishment, Implementation, Control & Improvement of IS Mgmt System
    - Based on BS 17799 Part 2 (Establishing & Maintaining a Security Program)
  - **27002:** Describes information security best practices (Based on BS 7799 Part 2)
    - Information Security Policy
    - Information Security Architecture
    - Asset management (classification & control)
    - Human resource security (Personnel)
    - Physical and environmental security
    - Communications and operations management
    - Access control
    - Systems acquisition/development & maintenance
    - Information security incident management
    - Business continuity management
    - Compliance
  - **ISO 27004**: Standard for security management measurements
  - **ISO 27005**: Assists with implementing information security based risk mgmt. approach
  - **ISO 27006**: Guide to certification/registration process
  - **ISO 27799**: Guide to protecting personal health information

Certification & Accreditation: (NIST 800-37)

- **Certification:** Detailed inspection verifying whether system meets documented security requirements
  - Inspects: Management, Operational, and Technical security controls
- **Accreditation:** The Data Owner's acceptance of the risk associated with the system & authorizing its implementation based on the discussed risks and security controls (may be performed by an auditor)
  - **Risk Owner:** Usually senior management. The person performing accreditation

Cryptography:

Encryption Services Provide:
Confidentiality: Denies unauthorized reads.
Authenticity: Validates the source of the message, to ensure that the sender is properly identified.
Integrity: Denies unauthorized writes - assurance that the message was not modified, accidentally or intentionally.
Non-repudiation: Establishes that a particular user performed a specific transaction, and the transaction did NOT change.

Terms & Definitions:
Cryptology: The science of secure communication
Cryptography: Secret Writing. Creating messages whose meaning is hidden
Cryptanalysis: The science of breaking encrypted messages (recovering their meaning).
Cipher: A cryptographic algorithm

Encryption: Process by which **plaintext** is converted to **ciphertext** with a **key,** using a cipher. (Encipher)
Decryption: Process by which ciphertext is converted to plaintext (with the key) by the use of a cipher. (Decipher)

Kerckhoff's Principle: Only the key should be kept secret. Algorithms should be publicly known.
Algorithm: Set of mathematical rules used in encryption and decryption
Key: Secret sequence of bits and instructions that governs the act of encryption and decryption
Work factor: Estimated time, effort, and resources necessary to break a cryptosystem

Diffusion: The order of the plaintext is dispersed in the ciphertext
Confusion: Creating a random relationship between the plaintext and the ciphertext
Substitution: Replaces one character with another, which provides diffusion
Permutation (Transposition): Provides confusion by rearranging the plaintext characters (like an anagram)
Modular Math: Shows what remains Y=25th letter. C=3rd letter. Y+C=B (b/c 25+3=28. 28-26=2 B=2nd letter)
XOR (Exclusive Or): Combining a key with a plaintext via XOR creates ciphertext (0+0=0 0+1=1 1+1=0 1+0=1)

Monoalphabetic Cipher: Uses ONE alphabet (A becomes X)
PolyAlphabetic Cipher: Uses two or more alphabets (A becomes X) (X becomes M) …
Running Key Cipher (Book Cipher): Substitution cipher using books, or some other known source. Agree on the source, then note the page#, line#, and word offset. Uses whole words at each position.
Scytale Cipher: Spartans. Wrap cloth around a rod and write down all the strips of cloth. Unwind to encrypt.
Caesar Cipher (Rotation Cipher): Monoalphabetic rotation cipher. Key is # of places to shift in alphabet (3: A=D)
Vigenere Cipher: Polyalphabetic cipher. Alphabet repeated 26 times in a Vigenere Square.
Cipher Disk: Two concentric disks, each with an alphabet around the periphery. Agree on key.
Jefferson Disks: 36 wooden disks, each with a scrambled alphabet along the edges. Write message on one line of the wheel and choose any other line of the wheels to be ciphertext. Recipient just looks for intelligible message.
Codebooks: Assign a codeword for important people, locations, and terms (i.e. The President is codeword Eagle)
One-Time Pad (Vernam Cipher): Unbreakable cipher. Key is as many bits as message. Key Mgmt issues.
Steganography: Hiding or embedding data (not encrypting) in an image.
Digital Signature: A hash value encrypted with a private key
Digital Certificate: A public key signed with a digital signature

Methods of Encryption:
Symmetric Encryption: Same exact key used to encrypt and decrypt (called: Secret key, Shared Key, Session Key)
- Examples: DES, TDES, AES, Twofish, RC6, Rijndael, MARS, Serpent
- Strengths: Performance
- Weaknesses: Key management

Asymmetric Encryption (PKI): Public and Private keys. One used to encrypt, another to decrypt.
- Examples: Diffie Hellman, RSA, ECC, El Gamal
- Requires: Digital Certificates, a Certificate Authority, a Registration Authority, and Trust

Strengths: Key management and digital signature support
Weaknesses: High computation cost, low performance.

Hybrid Encryption: Using Symmetric to encrypt the message, and Asymmetric to encrypt the symmetric key.

Hashing: One-way encryption using an algorithm, but NO KEY. Variable length input, fixed length output
Examples: SHA-1, SHA-2, MD5, MD6
Uses: Encrypting passwords in a database

Attribute	Symmetric	Asymmetric
Keys	One key is shared between two or more entities.	One entity has a public key and the other entity has a private key.
Key exchange	Out-of-band through secure mechanisms.	Public key is made available to everyone and private key is kept secret to the owner.
Speed	Algorithm is less complex and faster.	Algorithm is more complex and slower.
Use	Bulk encryption, which means encrypting files and communication paths.	Key distribution and digital signatures.
Security service provided	Confidentiality.	Authentication and nonrepudiation.

Cyrptographic Laws:
COCOM (Coordinating Committee for Multilateral Export Controls): Controlled the export of critical technologies, including cryptography, to the Iron Curtain countries during the cold war.
Wassenaar Arrangement: Included many former soviet countries and relaxed the restrictions on exporting crypto.

Encripherment Modes:
Block Mode: Message broken into blocks and each block is encrypted separately (susceptible to replay and substitution attacks).
Block Chaining: Parts of the previous block are inserted into the current block (not as susceptible to replay and substitution attacks).
Stream Cipher: Message broken into characters or bits and enciphered with a "key stream" (RC4, DES OF)

DES Modes:
ECB (Electronic Code Book): Block mode. No IV. No Chaining. Weak. Doesn't destroy patterns
CBC (Cipher Block Chaining): Block mode. Uses IV and Chaining. Errors propagate
CFB (Cipher Feedback): Stream mode. Uses IV and Chaining. Errors propagate.
OFB (Output Feedback): Stream mode. Uses IV and Chaining. Errors Don't propogate
CTR (Counter Mode): Stream mode. Uses IV and Chaining. Errors Don't propogate. Parallel processing

Symmetric Algorithms: Same key used to encrypt & decrypt. Requires key to be shared with recipient.
DES: Keys: 56-bit | Blocks: 64-bit | 16-rounds | Symmetric
TDES: Keys: 168-bit | Blocks: 64-bit | EDE or EEE | Symmetric
IDEA: Keys: 128-bit | Blocks: 64-bit | Symmetric
AES: Keys: 128, 192, 256 | Blocks: 128-bit | 10,12,14-rounds | Symmetric
RC5: Keys: 2048-bit | Blocks: 32, 64, 128-bit | Symmetric
RC6: Keys: 128, 192, 256-bit | Blocks: 128-bit | Symmetric
Blowfish: Keys: 32-448-bit | Blocks: 64-bit | Symmetric
Twofish: Keys: 128-256-bit | Blocks: 128-bit | Symmetric

Asymmetric Algorithms: Rely on one-way mathematical functions
Factoring Prime Numbers: prime x prime = composite (easy). Composite = prime? x prime? (hard)
Discrete Logarithm: (opposite of an exponent). 96,889,010,407 is what to what power? (hard)

Diffie-Helmann: Key Exchange or Key Agreement protocol. (discrete logarithm)
El Gamal: (discrete logarithm)
ECC (Eliptical Curve Cryptosystem): Asymmetric. Highest strength/bit of PKI. Lowest computation cost
RSA: Asymmetric.

Hashing Functions: Use an algorithm, but NO key to encrypt one-way. A variable length plaintext input is hashed into a fixed-length output (called a 'hash value' or 'message digest')
MD5: 128-bit output. Most widely used hashing algorithm, but being replaced by MD6
SHA (Secure Hash Algorithm): SHA-1: 160-bit output | SHA-2: 224, 256, 384, or 512-bit output
HAVAL (Hash of Variable Length): 128, 160, 192, 224, or 256-bit output

Algorithm Type	Encryption	Digital Signature	Hashing Function	Key Distribution
Asymmetric Key Algorithms				
RSA	X	X		X
ECC	X	X		X
Diffie-Hellman				X
El Gamal	X	X		X
DSA		X		
LUC	X	X		X
Knapsack	X	X		X
Symmetric Key Algorithms				
DES	X			
3DES	X			
Blowfish	X			
IDEA	X			
RC4	X			
SAFER	X			
Hashing Algorithms				
Ronald Rivest family of hashing functions: MD2, MD4, and MD5			X	
SHA			X	
HAVAL (variable-length hash values using a one-way function design)			X	

Cryptographic Attacks:
Brute Force: Generates the entire keyspace (every possible key) and tries them one at a time
Known Plaintext: Recovers and analyzes a matching plaintext and cyphertext pair to derive the key used

Chosen Plaintext: Cryptanalyst selects the plaintext to be encrypted, hoping to derive the key
Chosen Ciphertext: Crytpanalyst chooses cyphertext to be decrypted and uses docs signed with the public key
Meet-in-the-Middle attack: Encrypts on one side, decrypts on the other and meets in the middle. Attacker uses a known plaintext, gains the ciphertext, and tries to derive the key.
Known Key: Cryptanalyst knows something about the key, but not the key itself.
Differential Cryptanalysis: Seeks to find the difference between two related plaintexts that have been encrypted.
Linear Cryptanalysis: A known plaintext attack where cryptanalyst uses large amounts of plaintext/ciphertext created with the same key, to derive the key.
Side-Channel Attacks: Use physical data to break a cryptosystem. Monitor CPU cycles or power consumption
Birthday Attack: Named after the birthday paradox. Attacker attempts to find two plaintexts that result in the same ciphertext (called a collision).

Key Management:
-The key length should be long enough to provide the necessary level of protection.
-Keys should be stored and transmitted by secure means.
-Keys should be extremely random and the algorithm should use the full spectrum of the keyspace.
-The key's lifetime should correspond with the sensitivity of the data it is protecting.
-The more the key is used, the shorter its lifetime should be.
-Keys should be backed up or escrowed in case of emergencies.
-Keys should be properly destroyed when their lifetime comes to an end.

Digital Signatures: A hash value encrypted with a private key. Provides Nonrepudiation Authentication & Integrity. Used to cryptographically sign documents, email messages.
To digitally sign an email:
Sender:
Write email plaintext message
Run hashing algorithm on plaintext message to get hash value (aka message digest value)
Creates digital signature (encrypts the hash with his Asymmetric private key)
Attach the digital signature to the plaintext email and send
Receiver:
Receives email
Runs same hashing algorithm on email to get hash value (aka message digest value)
Decrypts digital signature with sender's public key
Compares receiver hash value with sender hash value to verify authenticity and integrity
Digital Certificate: (Provide Authenticity & Integrity) A public key signed with a digital signature. Std.= x.509.
Certificate Contents: Version#, Serial#, digital signature info, Issuer info, signer info
Registration Authority (RA) Accepts registration application and verifies authenticity of applicant
RA tells Certificate Authority (CA) to generate a digital certificate
CA hashes the digital signature, gets message digest value, & digitally signs that with their private key

HMAC (Hashed Message Authentication Code): (provides: Integrity & Authenticity)Combines symmetric encryption with hashing. Used by IPsec.
CBC-MAC (Cipher Block Chaining Message Authentication Code): (provides Integrity, Authentication, and Data Origin) Uses CBC block encryption to create MAC.

Link Encryption vs. End-to-End Encryption:

End-to-End encryption: Most familiar. Data/payload is encrypted, but not header/routing information.

Encrypted at the source, decrypted at the destination.

Link Encryption: Data/payload and header/routing info are both encrypted. Each hop must decrypt the message, read header info, encrypt, and send to next hop (each hop must have key). Used in Satellite communication.

Encryption at Different Layers

In reality, encryption can happen at different layers of an operating system and network stack. The following are just a few examples:

- End-to-end encryption happens within the applications.
- SSL encryption takes place at the transport layer.
- IPSec encryption takes place at the network layer.
- PPTP encryption takes place at the data link layer.
- Link encryption takes place at the data link and physical layers.

Email Security:
S/MIME (Secure Multipurpose Internet Mail Extensions): Standard mail format. Uses PKI to encrypt
PGP (Pretty Good Privacy): Asymmetric cryptosystem. Provides: Confidentiality, Integrity, Authentication, and Nonrepudiation). Used to encrypt email, docs, or hard drives. Uses "web of trust" model instead of using a CA.

Internet Security:
SSH (Secure Shell): Secure remote access. Preferred over unsecure Telnet and Unix R-Utilities.
SSL: Provides Authentication and Confidentiality to web traffic
TLS: Successor to SSL. Used to secure: web, email, and chat

IPSEC (Internet Protocol Security): Add cryptographic layer to IPv4 & IPv6.
OSI Layer: 3
Protocols:
AH (Authentication Header): Provides Authentication & Integrity for each data packet
ESP (Encapsulating Security Payload): Provides Confidentiality by encrypting the data
Modes:
Transport Mode: Only the payload/data is encrypted. Typically uses both AH and ESP.
Tunnel Mode: The entire IP packet, including headers, is encrypted. Typically uses only ESP.
SA (Security Associations): 2 per tunnel (directional). Includes lifetime, mode, MTU, algorithm, etc.
ISAKMP: Manages the SA process
IKE: Negotiates algorithm selection process.

Escrowed Encryption: Divides private key into two or more parts, which are held in escrow by trusted 3rd parties

Application & Systems Development:

Terms & Definitions:
Procedural Languages: Programming languages using subroutines, procedures & functions
Object-Oriented Languages: Treats a program as a series of connected objects the communicate via messages
Machine Code (Machine Language): Software executed directly by the CPU (Binary)
Source Code: Programming language instructions written in text that must be translated to binary before execution
High-Level Languages: Contain English-like instructions [Fortran]
Assembly Language: Low-level programming language (ADD, SUB). An assembler coverts it to binary
Compilers: Take source code (such as C or Basic) and compile it into machine code (binary executables)
Compiled Languages: The source code is compiled once and stored and run compiled.
Interpreted Languages: The source code (shell code) is compiled on the fly each time the program is run
Closed-Source Software: Released in executable form to keep source code confidential
Open-source Software: Source code is published so anyone can inspect, modify, and/or compile it.
Free Software: Gratis= free of charge | Libre= free to use how you choose
Verification: Checking to see if the system meets the detailed specifications
Validation: Checking to see if the application meets the high-level requirements
Certification: Formal technical verification by QC
Accreditation: Formal validation of overall security and functionality by management
Assurance: Verification that the implemented security measures work as designed
Software Escrow: 3rd party stores an archive of computer software. Used when a proprietary software vendor wants their code to remain secret, but the buyer wants assurance that they can have software if vendor closes doors

Software Development Models/Methods:

- **Waterfall:** Linear model with rigid, sequential phases. Unmodified Waterfall= No going back
  - Requirements
  - Analysis
  - Design
  - Code
  - Testing
  - Operations
  - (Destruction) Missing from Royce's model, but crucial
- **Sashimi**: Like waterfall, but steps overlap and you can go back a step. Each step validates the previous
- **Spiral:**
  - Designed to control risks.
  - Repeats the steps of a project over and over, increasing scope/complexity each time.
  - A risk analysis is performed at each round, increases the change of a risk being identified early
  - Each spiral round is considered a different project & can use a different software development methodology (ex. Waterfall)
- **Clean Room:** Increased design time to prevent defects , rather than removing them later.
- **Agile Software Development:**
  - **Scrum:** Teams hand off work to other teams as completed. Scrum Team lead by Scrum Master
  - **(XP) eXtreme Programming:**
    - Pairs of programmers working off a detailed specification
    - Heavy customer involvement
    - Improves: communication, simplicity, feedback, respect, courage
    - Core Practices: Planning, Paired Programming, Cust Involvement, Detailed testing
  - **RAD (Rapid App Development):**
    - Rapidly develop software using prototypes (dummy GUIs, DBs, etc.)
    - Goal= Quickly meet business needs of system. Technical concerns are secondary
    - Heavy customer involvement
    - Uses CASE tools, code generators, object-oriented techniques, etc. for effeciency
  - **Prototyping:**
    - Less time consuming than waterfall.

- Iterative approach – breaks projects into smaller tasks
- Uses mockups (prototypes) of system design features
- Produces a basic prototype that evolves each round

SDLC (secure Systems Development Life Cycle): [NIST 800-14] Used throughout the IT industry. Security is part of Every Step of the "Secure" SDLC.

- **Prepare Security Plan:** ensure security is considered/accomplished during each phase
- **Initiation:** the need and purpose of a system is documented
  - **Sensitivity Assessment:** determine level of sensitivity for information and system
- **Functional Design Analysis and Planning**
- **System Design Specifications**
- **Development/Acquisition:** system is designed, purchased, programmed, or developed
  - **Determine Security Requirements:** access controls, assurances, operational practices, etc.
  - **Incorporate Security Requirements into Specifications:** Ensure security items in project plan
  - **Obtain System and Related Security Activities:** develop security features, monitor threats, etc.
- **Implementation/Testing: i**nstall and test the system
  - **Install/Enable Controls: e**nabling/configuring/installing security controls
  - **Security Testing:** used to certify the security level of a system/application
  - **Accreditation:** formal authorization by management for system operation and risk acceptance
- **Operations/Maintenance:** system hardware/software changes
  - **Security Operations and Administration:** patching, user administration, key management, etc.
  - **Operational Assurance:** ensures operation complies with security requirements
  - **Audits and Monitoring:** security evaluation
- **Disposal:** secure decommissioning of a system
  - **Information:** move, archive, discard, destroy
  - **Media Sanitization:** overwrite, degause, destroy

OOP (Object-Oriented Programming):

- Objects (black boxes) have functions and methods for accomplishing certain tasks
- Saves time and money by reducing development time.
- Highly modular and self-contained.
- Provides encapsulation (data hiding). Users don't know how objects perform their work
- Examples: Java, C++, Smalltalk, Ruby
- **OOA/OOAD (Object-Oriented Analysis & Design)**
  - Flowchart showing the way data in a program flows & is manipulated
  - Visualized as a series of messages & objects
  - Seeks to understand a problem domain (challenge you're addressing) & designs the solution
  - Once OOA/OOAD is completed, an OOP language is used to write the code
- **OOP Concepts:**
  - **Class**: User-defined data types
  - **Objects**: An instance of a base class. Inherits methods and properties & has values for properties
  - **Methods**: Commands defined in a base class and inherited/performed by objects.
  - **Messages**: How objects communicate. Input & output to an object. Requesting/responding 2 calls
  - **Inheritance**: Inheriting methods and properties from a parent class
  - **Delegation**: Sending a function it doesn't understand to another object
  - **Polymorphism**: (many forms) Performs different operations depending on the message context
  - **Polyinstantiation**: (many instances) Two or more instances with the same name, different data
  - **Coupling**: Highly coupled objects require a lot of other objects to perform basic jobs
  - **Cohesion**: High cohesion objects are more independent. Low cohesion=high coupling

ORB (Object Request Brokers): Are used to locate objects (search engines for objects). Act as middleware.

- **COM** (Component Object Model): Locates objects on a local system. Allows objects written in different languages to communicate. Hides details of an individual object – focuses on capabilities.
- **DCOM** (Distributed Component Object Model): Like COM, but works over networks
- **CORBA** (Common Object Request Broker Architecture): Open vendor-neutral networked ORB. It separates the interface (communication syntax) from the instance (specific object)

(CASE) Computer-Aided Software Engineering:
Uses programs to assist in creating and maintaining other programs. Adds software to programming team.

- **Tools**: Support a specific task in the software-production process
- **Workbenches**: support one or few several process activities by integrating several tools in one application
- **Environments**: Support the software production process with a collection of Tools & Workbenches

Programming Language Generations:

- **First –** Machine language (01011010011) [Binary]
- **Second –** Assembly Language (al, 061h) [Assembly]
- **Third –** High-Level Languages (printf) [COBOL, C, Basic]
- **Fourth –** Very High Level (select * from). Increase programmer efficiency [ColdFusion, Oracle Reports]
- **Fifth –** Natural Language (father(x,y))

Top-Down (TD) Programming:

- Starts with broadest, highest level requirements and works down
- Procedural Programming languages (ex. C) typically use TD programming
- Risk: Incorrect assumptions can be made on performance of low-level devices

Bottom-Up (BU) Programming:

- Starts with low-level technical implementation details & works up (Define procedures first)
- Object-Oriented languages typically use bottom-up design (define objects and use to build program)
- Risk: Time wasted programming features that won't be used

Software Testing Methods:

- **Static Testing:** Passively tests code while not running. Walkthroughs, syntax checks, code reviews, etc.
- **White Box Testing:** Tester has access to source code, data structures, etc
- **Black Box Testing:** Tester has no internal details. Software is treated as a black box
- **Requirements Traceability Matrix:** Maps customer requirements to software testing plan

Software Testing Levels:

- **Unit Testing:** Low-level testing of software components, such as functions, procedures, or objects
- **Installation Testing:** Testing software as it is installed and first operated
- **Integration Testing:** Testing multiple components of a combined system
- **Regression Testing:** Testing software after updates, modifications, or patches
- **Acceptance Testing:** Testing to ensure software meets customer operational requirements
- **User Acceptance Testing:** Acceptance testing performed by the user
- **Fuzzing:** Random, malformed data packets are sent to program to see if it crashes. Programs that crash when receiving unexpected input probably have boundary checking issues (Buffer Overflow vulnerable)
- **Combinatorial Testing:** Black-box method testing all unique combinations of software inputs

Software Vulnerabilities:
This list is based on (CWE) Common Weakness Enumeration dictionary, by MITRE

- **Hard-Coded Credentials:** Backdoor username/passwords left by programmers in production code.
- **Buffer Overflow:** Occurs when a programmer does not perform variable bounds checking.
- **SQL Injection:** Manipulation of a back-end SQL server via a front-end web server.
- **Directory Path Traversal:** Escaping from the root of a web server into the regular file system ../..
- **PHP Remote File Inclusion (RFI):** Altering normal PHP URLs and variables to execute remote content
- **Cross-Site Scripting (XSS):** 3rd party execution of web scripting languages within the security context of a trusted site.
- **Cross-Site Request Forgery (CSRF/ XSRF):** 3rd party redirect of static content within the security context of a trusted site.

Types of Attacks:

- **Salami Attack:** Small amounts of fraud at a time
- **Data Diddling:** Unauthorized data modification over time
- **Logic Bomb:** Time or Event-based execution of malicious code
- **Validation Errors:** Not doing input validation, causing SQL injection and the like
- **Mistakes:** Software bugs that open vulnerabilities
- **Viruses:** Hook onto executable code (applications). Require user interaction to spread
- **Worms:** Self-propagating, don't need to attach to an application, and don't need user interaction to spread
- **Trojan Horse:** Malware masquerading as a useful program. Persistent backdoor access for attacker
- **Rootkit**: Malware focused on hiding its existence. Hides file, folder, process & network connection

Covert Channels:

- **Trap Door:** Hidden software or hardware mechanism that allows security to be circumvented
- **Back Door:** Installed by hackers to gain access
- **Covert Storage Channel:** Writing to storage by one process and reading by a lower security process
- **Covert Timing Channel:** One process signaling another process using system resources

Disclosure: The actions taken, by the discoverer, after a software vulnerability is discovered

- **Full Disclosure:** Releasing directly to the public, for awareness and to apply pressure for a hotfix
- **Responsible Disclosure:** Releasing to the vendor without notifying the public

CMM (Software Capability Maturity Model):

Framework for evaluating and improving the software development process
Strives for quality software and measurable, repeatable results.

5 Levels of CMM:

1. **Initial**: The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort.
2. **Repeatable**: Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
3. **Defined**: The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. Projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
4. **Managed**: Detailed measures of the software process and product quality are collected, analyzed, and used to control the process. Both the software process and products are quantitatively understood and controlled.
5. **Optimizing**: Continual process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

OLTP (Online Transaction Processing):

High performance and high availability programs that manage high volume transaction-oriented applications

- **Atomicity**: Divides transactions into units of work. All mods must take affect or all will roll back
- **Consistency**: Transactions follow integrity policy
- **Isolation**: Transactions are isolated from one another until completely processed
- **Durability**: Once verified as accurate, it is committed and can't be rolled back

Databases:

Structured collections of related data that allows queries, insertions, deletions, etc. Managed by DBMS.
DBMS (Database Management System): Controls access and enforces database security

Database Types:

- **Object-Oriented:** Persistent objects and procedures stored in a DB
- **Hierarchical:** Tree structure with parent-child relationships
- **Network:** Represents objects and their relationships
- **Distributed Data:** Data stored in more than one DB with logical links
- **Relational Databases:** (Most Common) SQL: 2-dimensional tables of related data

- **Table**= Relation
- **Tuple**= Row
- **Attribute**= Column
- **Value=** A Single Cell
- **Primary Key**= Unique value, used for identification per Row/Tuple
- **Foreign Key**= Matches the primary key in the parent DB. Used for joining tables

Data Integrity: Ensures the integrity (correctness) of the table data

- **Referential Integrity:** Every foreign key in a secondary table matches a primary key in the parent table
- **Semantic Integrity:** Every attribute (column) value is consistent with the attribute data type
- **Entity Integrity**: Every tuple (row) has a unique primary key that is not null
- **Data Integrity**: The overall integrity of the entries in a database. Protection from unauthorized changes

Database Normalization: Removes redundant data and improves database integrity.

- **First Normal Form (1NF):** Divide data into tables
- **Second Normal Form (2NF**): Move data that is partially dependent on the primary key to another table.
- **Third Normal Form (3NF):** Remove data that is not dependent on the primary key.

Database Query Languages:

- **DDL** (Data Definition Language): Used to create, modify, and delete tables
- **DML** (Data Manipulation Language): Used to query and update table data

Database Security Issues:

- Confidentiality and integrity of stored data
  - Integrity is primary concern when replicated databases are updated
- **Aggregation**: Combining low-sensitivity data to identify highly-sensitive data
- **Inference**: Deducing or inferring information beyond one's level of access
- **Polyinstantiation**: Creating different sets of tuples for different classification levels

Database Views: Used to provide a constrained interface (limited access). Also, the result of a database query
Data Dictionary: Describes database tables, database schema, access, etc. For developers to use
Data Warehouse: Multiple databases pulled into one & normalized for data mining
Data Mart: A temporary, tactical data warehouse created for a specific purpose

Database Replication and Shadowing:

- **Database Replication:** Mirrors a live database, allowing simultaneous client-generated reads and writes to all replicated databases
- **Shadow Database**: Mirrors all changes made to the primary, but clients can't access it. All data is sent from the live database to the shadow database.
- **Database Journal:** Log of all database transactions. Transaction logs can be replayed after a restore

Data Interface Languages:

- **ODBC** (Open Database Connectivity): Standard API for database access
- **OLE DB** (Object Linking and Embedding): Microsoft COM-based API for data access
- **ADO** (ActiveX Data Objects): Microsoft simplified OLE DB for data access
- **JDBC** (Java Database Connectivity): Sun API for Java access to databases
- **XML** (eXtensible Markup Language): W3C standard for structured data

Knowledge-Based Systems:

- **Artificial Intelligence**:
  - **Expert Systems:** Inference engine analysis, fuzzy logic analysis, probability.
    - Knowledge Base: If/Then statements used to make decisions
    - Inference Engine: Follows the tree formed by knowledge base & fires on mismatch
  - **ANN** (Artificial Neural Network): Axon, Synapses, Post-synaptic-potential.

- **Bayesian Filter:** Formula for calculating conditional probabilities
- **Genetic Algorithms:** Generates a population of random programs, Executes each and assigns it a fitness value, create a new population of programs using the best attributes of the first group, etc.

Operations Security:

Terms & Definitions:
Operations Security: The security of all applications, systems, network and processes. Begins once the network is in place and constantly evolves as a result of new threats, new regulations, and changes in operational methodology.
Due Care: Taking careful actions that a "prudent person" would take under similar circumstances
Due Diligence: The amount of investigative effort a "prudent person" would utilize to make a business decision
Prudent Person: A person of normal mind (responsible, careful, cautious, practical person)
Collusion: An agreement between two or more people to subvert security
Remanence: Data that might persist after removal attempts
RAID: A method of using multiple disk drives to increase reliability, speed, or both
Mirroring: Complete duplication of data to another disk (on same drive controller)
Duplexing: Complete duplication of data to another disk on another disk controller
Striping: Spreading data writes across multiple disks, to increase performance
Baselining: Capturing a point-in-time snapshot of a system's security configuration. Should be done periodically
Configuration Management: Developing a consistent system security configuration (Security Templates)
Change Management: Process to understand, communicate, and document any changes to systems
Vulnerability Management: Includes vulnerability scanning and managing mitigation of vulnerabilities
Zero-Day Vulnerability: A vulnerability is known before the patch exists
Zero-Day Exploit: Exploit code for a vulnerability is available before the patch exists
(SLA) Service Level Agreement: Stipulates all expectations of behaviors, services, and quality of services

Role of the Operations Department:

- Operations security is about people, data, media, hardware, and the threats associated with each of these in a production environment.
- Ensure due care is taken to protect information assets
- Shows due diligence in creating and enforcing policies, procedures, standards & guidelines
- Focuses on the protection of assets, not simply meeting legal or regulatory requirements. A company may be complying with legal and regulatory requirements and still not be practicing due diligence & due care
- Ensures controls are in place to prevent people from inadvertently or intentionally compromising the confidentiality, integrity, or availability of data or the systems and media holding it

Administrative Management:

Ensures controls are in place to inhibit people from inadvertently or intentionally compromising the CIA of data or systems and the media holding the data. Controls people's operational access to data.

** If a control has a negative ROI, and it isn't a legal or regulatory requirement, it should Not be implemented**

- **Least Privilege:**
  - Administrative, Preventive control
  - Reduces risk through limiting access to the minimum necessary access
  - Only provides rights & access to information necessary to perform their job responsibilities
  - Primarily applies to Discretionary Access Control, but also applies to Mandatory Access Control
- **Need to Know:**
  - Administrative, Preventive control
  - Used in Mandatory Access Control environments to further enhance security
  - MAC makes access determinations based on the clearance level of the subject and the object's classification. Need to Know goes one step farther to require subject not only have the appropriate clearance level, but have a need to know
  - Uses Compartmentalization to enforce need to know.
- **Separation of Duties**
  - Administrative, Preventive control
  - Multiple people required to complete critical or sensitive transactions
  - Requires collusion to compromise security
  - Reduces risk of fraud and error
  - Increases accountability

- **Job Rotation / Rotation of Duties:**
  - Administrative, Detective & Deterrent control
  - Requires that critical job functions aren't continually performed by the same one person
  - Can detect fraud behavior and reduce the risk of burn out
- **Mandatory Vacations:**
  - Administrative, Detective & Deterrent control
  - Allows for detection of unauthorized activity while the person is on vacation
  - Prevents burn out
  - Identifies area where depth of job coverage is lacking
- **Accountability**:
  - Administrative Control
  - Use of audit logs & other controls to ensure accesses are properly managed
  - Looks for appropriate or inappropriate access to restricted data, and repetitive errors
  - Must be reviewed on a routine basis
- **(NDA) Non-Disclosure Agreement:**
  - Administrative, Directive control
  - Contractual agreement, signed before sharing, to maintain confidentiality of sensitive information
  - All employees, outside contractors/consultants, and third parties receiving info should sign one
- **Background Checks / Pre-employment Screening:**
  - Administrative, Preventive control (Pre-employment)
  - Administrative, Detective, Deterrent (ongoing random checks)
  - The sensitivity of the position being filled usually dictates the depth of the investigation
- **Privilege Monitoring:**
  - Detective control
  - Monitoring the actions of those with privileged access to critical systems & sensitive data

Assurance Levels:

- **Operational Assurance**
  - Focuses on product architecture, features & functionality
    - Is the product performing as promised? If not, is it incapable or poorly configured?
  - Areas to consider when evaluating products
    - Access control mechanisms
    - Separation of privileged and user program code
    - Auditing and monitoring capabilities
    - Covert channel analysis
    - Trusted Recovery
- **Life Cycle Assurance**
  - Focuses on how the product was developed and how it will be maintained
    - Design specifications
    - Clipping-level configuration
    - Unit and integration testing
    - Configuration management
    - Trusted distribution
  - Who is responsible for ensuring the system is maintained?
    - Patching
    - Routine maintenance

Operational Responsibilities:

- **Implement safeguards and countermeasures to protect resources, information, and hardware**
- **Asset identification & management** (servers, desktops, laptops, printers, network hardware, etc.)
- **Establishment & management of system controls** (processes at appropriate security level, etc.)
- **Prevent recurring problems**
- **Reduce hardware and software failures**
- **Reduce impact of incidents or disruption**
- **Investigate unusual occurrences, deviations from service levels, or abnormal conditions**

- **Diagnose problems using all available resources (ex. system logs, network monitors, etc.)**
- **Identify logical solutions for problems**
- **Change control**
  - Track and manage All changes in systems and facilities (works with configuration management)
  - Change mgmt policy includes: Type of change, who is making, who approved & change detail
  - Change control: reduces risk & recovery time, and improves forensic investigation of incidents
- **Remote Access Security**
  - Use a secure transmission medium (SSH, IPSEC, VPN, etc.)
  - Administer critical systems locally
  - Limit number of people with remote access
  - Use strong authentication (two-factor)
- **System hardening**
  - Take appropriate physical security actions to protect systems
  - Helps protect against zero-day attacks by reducing the attack surface of a system to the required
  - Disable unnecessary services, remove extraneous programs, enable security capabilities, etc.
  - Encrypt data (ex. whole disk encryption)
  - Control data flow to removable media
  - Disable or uninstall unnecessary services
  - Close unnecessary ports
  - Apply patches and updates
  - Manage service/system accounts
- **Input & output controls**
  - Application testing must be performed to ensure only valid input can be entered
  - Output should have proper access control for all data, be sent to appropriate receiver, etc.
- **Trusted recovery**
  - System should Not fail in an insecure state
  - Reason for failure is typically:
    - Insecure transaction
    - Transaction not understood
  - System should react to protect itself by:
    - System reboot: After a controlled shutdown in response to TCB failure
      - Caused by: Insufficient resources to continue, inconsistent data
    - Emergency system restart: After an Uncontrolled shutdown
      - Caused by: kernel failures, media failures, users illegal attempts
    - System cold start: When a system fails & can't recover to a stable and secure state through a system reboot or emergency restart.
      - May require administrative intervention to correct the problem
- **After a system crash**
  - Enter single mode (doesn't fully load services, but allows admin recovery)
  - Fix issue and recover files
    - Salvage file system
    - Identify cause
    - Roll back or roll forward databases
    - Manually return system to full use mode
    - Validate critical files and operations

Change Management: Process to understand, communicate, and document any changes to systems

- **Change Management Flow:**
  - Identify a change
  - Propose a change
  - Assess the risk associated with a change
  - Test a change
  - Schedule a change
  - Notify impacted parties
  - Implement a change

- Report results

- **Change Control Process:**
  - Process to track & manage change in systems and facilities (Works with configuration management)
  - Reduces risk by reducing Outages, Vulnerabilities, and Errors
    1. **Request for change to take place**
       a. Presented to person/group responsible for making change
    2. **Approval of change**
       a. Benefits of change clearly established, change justified, and pitfalls identified
    3. **Documentation of change**
       a. Entered into change log
       b. Continually updated as process continues
    4. **Tested and presented**
       a. Changes must be fully tested & may need to be presented to a change committee
    5. **Implementation**
       a. Develop a schedule
    6. **Report to change management**
       a. Report summarizing the outcome of the change (success or failure)

    All Changes should be tracked/audited and should include a back out plan

Sensitive Information / Media Security Controls:

- Ensure the CIA of data on media (primary storage, backup storage, etc. wherever it exists)
- Create processes to ensure data is not destroyed, inaccessible (Avail), disclosed (Conf), or altered (Int)
- **Labeling**: Media should be labeled (Classification, create date, creator, retention period, name, version)
- **Handling**: Media should only be handled by trusted individuals.
- **Logging**: The handling of media should be logged
- **Encryption**: Media should be encrypted, to prevent unauthorized disclosure (Confidentiality)
- **Retention**: Media should not be retained past useful life or legal requirement. Librarians retain media
- **Sanitize**: Media should be Sanitized when its retention period has expired
  - **Erasing**- Leaves files on media. Only removes pointers in FAT
  - **Purging**- Extremely difficult to recover
  - **Wiping, Overwriting, Shredding**- Overwrites each bit or block of file data
    - One successful pass is sufficient for businesses, but the DoD requires 3, 5, or 35 passes
  - **Zeroization**- Overwriting with a pattern
  - **Degaussing**- Magnetic scrambling
  - **Physical destruction**- (Most Secure) Hardware shredded, pulverized, or incinerated

Media Management:

1. Track
2. Implement access controls
3. Track versions
4. Track change history
5. Protect from environmental conditions
6. Ensure integrity of media
7. Inventory on scheduled basis
8. Execute secure disposal activities

Network & Resource Availability:

- **(MTBF) Mean Time Between Failures:**
  - Approximately how long a device will last
  - Determined by manufacturer or a trusted third party
- **(MTTR) Mean Time to Repair:**
  - How long it takes to repair a failure (can be time in an SLA)
  - Consider redundancy if MTTR is too high
- **Single Points of Failure**
  - May cause more failures across the network

    - Defenses:
        - Maintenance
        - Backups
        - Redundant Hardware (ex. 2 power supplies)
        - Redundant Systems (spare hardware)
        - High-Availability Clusters / Failover Clusters
        - Mirroring: Writes info to multiple disks on same controller
        - Duplexing: Writes info to multiple disks on different controllers
        - Direct Access Storage Devices: All points on disk can be reached
        - Sequential Access Storage Devices: All points must be accessed in sequence (Tapes)
- **RAID Levels:**
    - 0: Striped Set [No redundancy]
    - 1: Mirrored Set
    - 2: Hamming code parity (NOT Used today) [Requires 14 or 39 disks]
    - 3: Byte-level parity (dedicated (1 drive) parity)
    - 4: Block-level parity (dedicated (1 drive) parity)
    - 5: Interleave Parity (Striped Set with distributed (all drives) parity) (1 drive can be lost)
    - 6: Double Block-level Parity (RAID 5 with additional fault tolerance (2 drives can be lost))
    - 10: Striping and Mirroring (Striped set of mirrors)
- **Clustering:**
    - Server Cluster: Group of servers viewed as one. Load balancing
- **Grid Computing:**
    - Group of systems sharing their idle processor time
    - Not secure & not intended for time sensitive applications
    - Commonly used in modeling (financial modeling, weather modeling, etc.)
- **Backups**:
    - Backup Policy: What gets backed up, How often, When, How
    - Conduct periodic restores
    - Log backups (successes & failures)
- **Hierarchical Storage Management:**
    - Continuous online backup
    - Places data on storage devices based on amount of access

Hack & Attack Tools:

- Probes: Ping sweepers
- Port Scanners/Network Mapping: (NMap)
- Password Crackers (LophtCrack, John the Ripper)
- WiFi Finders (NetStumbler)
- Vulnerability Scanning Tools (Nessus)
- Exploit code deployment tools (MetaSploit)
- Packet capture/Sniffers (WireShark)

Hack & Attack Types:

- **(DoS) Denial of Service:** Land (same Src & Dest) | Smuf (ICMP flood) | Fraggle (UDP flood) | Teardrop
- **Man-in-the-middle:** Intruder injects himself into the middle of a conversation as an unknown proxy
- **Session Hijacking:** Compromising or seizing an existing network session
- **Ping of Death**: Oversized ping packets causing system to go down
- **Mail Bombing**: Overwhelming a mail server
- **Wardialing**: Seeking out modems in an organization
- **Teardrop**: Malformed fragmented packets causing systems to freeze
- **Password Guessing**: Online attack where attacker attempts to authenticate to a particular system
    - **Countermeasure**: Account Lockout | **Detective Control:** Clipping Level- Min alerting threshold
- **Password Cracking:** Offline attack where attacker has gained access to password hash or database

Vulnerability Testing:

- One part of ensuring networks are secure, but not an accurate indicator of security status by itself
- Only a snapshot in time
- Identifies: Weak account security, Open ports, Unnecessary services, Misconfigurations, etc.
- Before conducting:
  - Get written permission
  - Consider ramifications of conducting tests
  - Understand scope and goals
- Follow-up with a Penetration test to identify false positives

Penetration Testing:

- Simulates attacks against systems to determine their level of vulnerability
- **Pen Testing Steps:**
  - **Discovery:** Footprinting and gathering information about the target
  - **Enumeration**: Performing port scans and resource identification methods
  - **Vulnerability Mapping:** Identify vulnerabilities in identified resources
  - **Exploitation:** Attempting to gain unauthorized access by exploiting vulnerabilities
  - **Report to Management:** Delivering documentation of test findings & countermeasures to mgmt
- **Degrees of Knowledge:**
  - **Zero Knowledge:** Team must start from knowing nothing
  - **Partial Knowledge:** Team has some information about the target
  - **Full Knowledge:** Team has intimate knowledge of target
- **Forms of Testing:**
  - **Blind:** Assessor has only publicly available knowledge. Network/Security team is aware of test
  - **Double-Blind:** Assessor has only public knowledge. Network/Security staff is unaware of test
  - **Targeted:** Focused test (new system being rolled out, specific system, etc.)
- **Commonly Exploited Vulnerabilities:**
  - **Kernel Flaws:** Provide most powerful control over system
    - Countermeasure: Apply security patches
  - **Buffer Overflows:** Provide same level of system access that program had
    - Counter measure: Secure programming techniques
  - **Symbolic Links:** Used in Unix/Linux systems. "Stub file" redirects access to another place
    - Countermeasure: Code programs & scripts so full path can't be circumvented
  - **File Descriptor Attacks:** Provide elevated privileges. Numbers represent open files
    - Countermeasure: Secure programming practices
  - **Race Conditions:** Puts programs in vulnerable condition before it can be mitigated
    - Countermeasure: Secure programming practices
  - **File & Directory Permissions:** Improperly set authorization levels
    - Countermeasure: File integrity checkers
- **Post-Pen Testing:**
  - Provide a prioritized list of risks, and an interpretations/description of the risks
  - Develop risk mitigation plans
  - Track risk mitigation activities to ensure all risks are (Accepted, Mitigated, or Transferred)

Incident Response Management:

- A methodology for identifying and responding to security incidents, during or after they have occurred
- **Goal**: Control the cost and damage associated with incidents, and speed recovery of impacted systems
- **Event**: Any observable data associated with systems or networks
- **Incident**: When events suggest that violation of security posture has or is likely to occur
  - Ex. Policy violations, insider stealing customer credit card numbers, etc.
- **(CSIRT) Computer Security Incident Response Team:** The group that monitors, identifies, and responds to security incidents
- **Incident Response Phases:**
  - **Detection:** Analyzing events to determine whether they comprise a security incident
  - **Containment:** Contain to prevent further damage, and perform forensic backup of system(s)

- **Eradication:** Finding root cause and removing it
- **Recovery:** Restoring the system(s) to operational status (Ex. rebuild or restore from backup)
- **Reporting:** Detailed report on incident, to management, on lessons learned (prevent & respond)

Physical Security:

Terms & Definitions:
Mantrap: Preventive 2-door physical control. Each door requires separate form of authentication
Bollard: A post designed to stop a car, typically in front of building entrances
Smart Card: Physical access control device with integrated circuit
Tailgaiting: Following an authorized person into a building without providing credentials
GreenField: undeveloped lot of land
Object Rescue: The act of recovering information from previously used objects (files, tapes, etc.)
Deleting: Removes the entry from the FAT and marks the blocks unallocated (data remains)
Formatting: Destroys the FAT and creates new one (data remains)
Overwriting: Writes over every character of a file or disk (more secure)
Shredding/Wiping: Overwrites file data before removing the FAT entry
Degaussing: Destroys the integrity of magnetic media through using a strong magnetic field
Destruction: Physically damages the media itself (incenerating, pulverizing, acid bath, etc.)
****When in Doubt: Hire an Expert on Physical Security Matters****

Physical (Environmental) security Goal:
To protect the CIA of physical assets (people, buildings, systems & data)
Human safety is the most critical concern of the domain

Physical Controls:
- Physical: locks, fences, guards, mantraps, etc
- Administrative: Policy, Procedures, etc.
- Technical: biometric scanners, cameras, etc.

Perimeter Defenses:
- **Fences**: deterrent to preventative. Used to steer ingress/egress to controlled points (gates)
- **Gates**: Placed at controlled points of perimeter
    - Class 1: Residential use (ornamental)
    - Class 2: Commercial/General Access (parking garage)
    - Class 3: Industrial/Limited Access (loading dock for 18-wheeler)
    - Class 4: Restricted Access (airport or prison) - designed to stop a car.
- **Bollards**: Strong post designed to stop cars. Placed in front of physically weak areas (entryways)
- **Lights**: Detective/Deterrent control. Measured in Lumen (1 candle) or Lux (1 candle/sq meter)
- **CCTV**: Detective control to aid guards. Key issues: depth of field (in focus) and field of view.
- **Locks**: Preventive controls. May be mechanical or electronic (smart cards)
    - **Key Locks:** Different locks have different "attack times" (take longer to pick or bump)
        - **Pin tumbler locks:** require driver pins and key pins
        - **Warded locks:** must turn a key through wards (ex. Skeleton keys)
        - **Spring-bolt locks**: are like deadbolt locks, except the door can be closed with them extended.
    - **Combination Locks:** Dial, Keypad, or Push Button. Possible combinations = the pool of numbers multiplied by the number of positions (ex. Master dial lock has numbers 1-40 and has 3 positions (40*40*40= 64,000 possible combinations).
    - **Smart Cards and Magnetic Stripe Cards:** Used for electronic locks, credit card purchases, and dual-factor authentication systems. "Smart" cards have integrated circuits (also called ICC). May be contact (swipe) or contactless (RFID). CAC is one type.
- **Mantraps**: Preventive physical control with two doors, each requiring a different form of authentication to open. Requires safe egress
- **Turnstiles:** Prevent tailgaiting by enforcing one person per authentication. Requires safe egress
- **Guards**: Deterrent and Detective dynamic controls that can aid other security controls . Amateur guards should not be used where critical assets need protection.

- **Dogs:** Deterrent and Detective controls. Present legal liability
- **Walls**:
  - Should go from true floor to true ceiling
  - should have an appropriate fire rating (amount of time required to fail due to fire)
  - National Fire Protection Agency (NFPA) 75 states: Computer rooms should be separated from other occupancies by walls rated at no less than 1 hour

Attacks:
- **LockPicking**: The art of opening a lock without the key
- **Lock Bumping:** Inserting a shaved down key and hitting the exposed end with a screwdriver handle (or similar), causing the pins to jump, then quickly turning the key while the pins are in flight. The pins will eventually be caught in the correct position and the lock will open.
- **Piggybacking/Tailgaiting:** Inappropriately using the legitimate access of another person.

Motion Detectors and other Perimeter Alarms:
- **Ultrasonic and microwave motion detectors:** Send a wave of energy out and waiting for the echo to bounce off something and return
- **Photoelectric motion sensors:** Send a beam of light to a photoelectric eye, which alerts when the beam of light is broken
- **Magnetic window and door alarms:** sound the alarm when the electrical circuit between the magnets is broken

Drive and Tape Encryption:
Protection of data at rest is one of few controls that can protect data after a physical security breach
Whole disk encryption is preferred, b/c partial disk risks exposing temp files, swap file, etc.
Software-based encryption is slower but cheaper than hardware-based encryption
Sensitive backup data should be stored offsite (and handled end-to-end by a bonded, insured company)

Overwriting Data:
- **Deleting**: Removes the entry from the FAT and marks the blocks unallocated (data remains)
- **Formatting**: Destroys the FAT and creates new one (data remains)
- **Overwriting**: Writes over every character of a file or disk (more secure)
- **Shredding/Wiping**: Overwrites file data before removing the FAT entry
- **Degaussing**: Destroys the integrity of magnetic media through using a strong magnetic field
- **Destruction**: Physically damages the media itself (incenerating, pulverizing, acid bath, etc.)

Site Selection, Design, and Configuration:
Physical safety of personnel is the top priority when selecting, designing, and configuring a site. **Topography** can be used to steer ingress/egress to controlled points.
Utility reliability is critically important. Shared tenancy & shared demarks can pose security issues
Environmental Controls (Power, HVAC, and Fire Safety):
Recommended Temp and Humidity: Temp: 68-77F Humidity: 40-55%
Reliable electricity is one of top-10 priorities
Electrical Faults:
- **Blackout**: Prolonged power loss
- **Brownout**: Prolonged low voltage
- **Fault**: Temp power loss
- **Surge**: Prolonged high voltage
- **Spike**: Temp high voltage
- **Sag**: Temp low voltage

EMI (Electromagnetic Interference): All electricity generates magnetism, and creates EMI (network cables, power cables, circuits).

Fire Detection:

Smoke Detectors:

- **Ionization**: Radioactive source and a sensor. Trips when smoke interrupts radioactivity
- **Photoelectric**: Use an LED and a photoelectric sensor. Trips when smoke interrupts light

Heat Detectors:

- Alert when temperature exceeds an established safe baseline, or when the temperature increases at a specific rate (i.e. 10 degrees in 5 minutes)

Flame Detectors:

- Detect infrared or ultraviolet light emitted in fire. Requires line of sight to detect fire

Fire and Suppression Agents:

Fire Suppression Agent Classes:

A: Common combustibles (wood, paper, etc). [Water or Soda Acid]
B: Liquid (oil, alcohol, petroleum products). [Gas (Halon/FM200) or Soda Acid]
C: Electrical. [Gas (Halon/FM200)]
D: Metals. [Dry Powder]
K: Kitchen (grease, oil). [Wet Chemicals]

Recommended Fire Suppression Agent: **Water** (except electrical fires), b/c it is safest for people
Halon is no longer used b/c it damaged the ozone (Montreal Accord banned its use)
FM200, FE-13, Argon, and Inergen are a few suitable replacements.

Fire Extinguishers:

Wet Pipe: Water to sprinkler head. A glass bulb or metal melts, activating that sprinkler head
Dry Pipe: Pipes are filled with compressed air, and water replaces air when the heads activate
Deluge: Sprinkler heads are opened, and water fills pipes when a water valve is opened
Pre-Action: Require two separate triggers to release water.

Evacuation Roles & Procedures:

- **Safety Warden**: Ensures all personnel safely evacuate the building in an emergency or drill
- **Meeting Point Leader**: Assures all personnel are accounted for at emergency meeting point

HVAC:

- **Positive Pressure and Drains:** Air and water should be expelled & repelled from the building
- **Recommended Humidity:** 40-55%
  - **Low Humidity:** Causes static electricity **High Humidity:** Causes condensation
- **Recommended Heat:** 68-77 degrees farenheit (20-25 celcius)

Business Continuity & Disaster Recovery:

Terms and Definitions:

(BCP) Business Continuity Plan: Long-term & Business-Focused. Concerned with business-critical functions and services, not the systems/applications that allow that function to be performed. Long-term strategy to Ensure the business will continue to operate (critical business functions/services) before, during, and after a disaster is experienced. A BCP will contain: Crisis Communication Plan, Occupant Emergency Plan (OEP), Continuity of Operations Plan (COOP), Cyber Incident Response Plan, Continuity of Support Plan/IT Contingency Plan, Disaster Recovery Plan, Business Recovery Plan (BRP), and Disaster Recovery Plan (DRP).
(DRP) Disaster Recovery Plan: Short-Term, Tactical, IT-focused, plan to recover from a disruptive event. Goal= Efficiently mitigate disaster impact. DRP will be a part of the BCP.
Incident Management: Used for threats too small to include in the BCP and CP
(COOP) Continuity of Operations Plan: Plan to maintain operations during a disaster
(MTD) Maximum Tolerable Downtime: Critical (minutes to hrs) | Urgent (24-hrs) | Important (72-hrs) | Normal (7-days) | Nonessential (30-days).
(MTBF) Mean Time Between Failures: How long a new or repaired system will run before failing
(MTTR) Mean Time To Repair: How long it takes to recover a failed system.
(RTO) Recovery Time Objective: Time available to recover a disrupted system/resource
(RPO) Recovery Point Objective: Data loss tolerable by the business (6 days for weekly full backup)
(WRT) Work Recovery Time: After systems/resources are recovered, time to recover lost work/backlog
Preventive Measures: Reduce possibility of experiencing a disaster, and reduce impact of a disaster
Recovery Strategies: Processes on how to rescue the company after disaster strikes
Disaster: Disaster is declared when an interruption occurs and recovery will exceed MTD.

Business Continuity Planning: Pre-planned procedures that allow an organization to:

- ❑ Provide immediate and appropriate response to emergency situations
- ❑ Protect lives and ensure safety
- ❑ Reduce business impact
- ❑ Resume critical business functions
- ❑ Work with outside vendors during the recovery period
- ❑ Reduce confusion during a crisis
- ❑ Ensure survivability of the business
- ❑ Get "up and running" quickly after a disaster

Why spend the time, money, and effort doing a BCP?

- ❑ Loss of or injury to personnel
- ❑ Implications of Rules and Regulations
- ❑ Loss of Revenue
- ❑ Damage to Critical Resources
- ❑ Loss of Customers
- ❑ Civil and Criminal Liabilities
- ❑ Damage to Reputation

BCP life cycle stages: [memory aid: Initiation Impacts Preventive Recovery Contingency Testing]

- ❑ **Project Initiation**: Obtain Management Support, Develop the continuity planning policy statement, provide guidance to develop a BCP, and assign authority to the roles.
- ❑ **Business Impact Analysis (BIA):** Identify mission critical processes, analyzes impacts to business if these processes are interrupted as a result of a disaster. Considerations: Max tolerable downtime (RTO/Recovery Window), Financial impact, productivity impact, legal/regulatory requirements, and brand damage.
- ❑ **Identify Preventive Controls (Recovery Strategy)**: Preventive controls to mitigate known risks resulting from the BIA
- ❑ **Develop Recovery Strategies (Plan Design and Development):** Formulate methods to ensure systems and critical functions can be brought online quickly

- **Develop the Contingency Plan (Implementation):** Procedures and guidelines for for how the organization can stay functional in a degraded state
- **Testing the Plan, Training, and Exercises (Testing):** Identifies deficiencies, clarifies roles, allows team members to practice their roles.
- **Maintain the Plan (Continual Maintenance):** New threats? Business changes?

BIA Steps:
- Select individuals to interview for data collection
- Data Gathering (surveys, questionnaires, quantitative and qualitative approaches)
- Identify critical functions
- Identify resources needed to perform critical functions
- Calculate how long the functions can survive without these resources
- Identify vulnerabilities/threats to the functions
- Calculate the risk for the functions
- Document findings and report to management

BIA Report (summarized the following):
- List of Critical Processes
- List of MTD by process
- Criticality Rankings by function
- Prioritized list of systems and applications
- Prioritized list of non-IT resources
- List of RTOs
- List of RPOs

Disaster Classifications:
- Natural (hurricane, tornado, earthquake, etc.)
- Human [Most Common Classification] (includes technical (malware))
- Environmental (systems environment, NOT weather)

Recovery Strategies should be broken down into:
- Business process recovery
- Facility recovery
- Supply and technology recovery
- User environment recovery
- Data recovery

Facility Recovery:
- **Redundant Site:** Owned and maintained by the company. Mirrors production.
- **Hot Site:** Leased site with fully configured equipment (recover within hours)
- **Warm Site:** Leased site with partially configured equipment
- **Cold Site:** Leased site with basic environmentals, but no equipment
- **Reciprocal Agreement:** Mutual agreement with another company to use space & equip.
- **Rolling Hot-Site (MRU):** Trucks/units with necessary power & telecomm
- **Multiple Processing Center:** Call centers, service centers, etc. in different locations
- **Hardware Backups:** Purchase or Leased backup equipment for a disaster (cost vs. time)
- **Software Backups:** Full, Differential, and Incremental backups.

Data Backup Alternatives:
- **Electronic Vaulting:** Batch process. Writes all changed files to remote copy (full files)
- **Remote Journaling:** Real-time. Deltas only (journal or TLogs). Restore full then apply
- **Tape Vaulting:** Sending backup tapes to an off-site facility (manual or electronic)

Insurance: Fills gaps in preventive countermeasures, based on risks and threats identified in BIA
- **Cyberinsurance**: Insures against losses caused by denial-of-service attacks, malware damages, hackers, electronic theft, privacy-related lawsuits, etc.

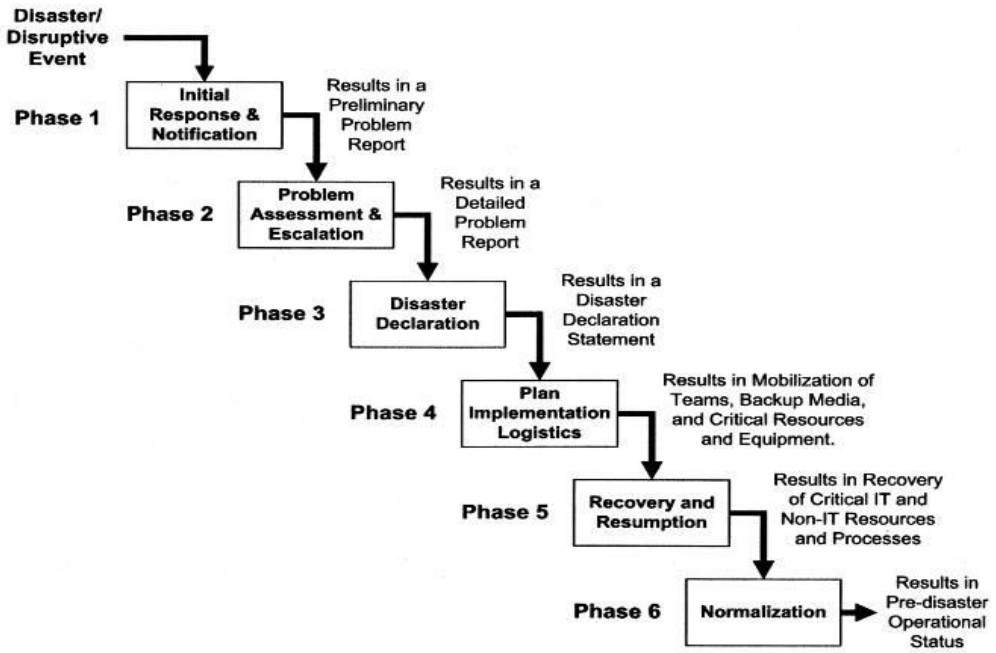
- **Business Interruption Insurance:** In the event the company is out of business for a certain amount of time, pays for specified expenses and lost earnings, outstanding accounts receivables.

Contingency Plan Teams:

- Damage assessment team
- Legal team
- Media relations team
- IT recovery team
- Relocation team (facilities)
- Restoration team
- Salvage team
- Security team

Reconstitution Phase: Company moves back to its old site, or a new site. The company is not out of its "emergency" phase until it is back in operations at the original or new primary site.

BCP Execution Phases:



Recovery / Testing Exercises:

- **Structured Walk-Through Exercise:** Occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan.
- **Checklist Exercise aka "Desk check" test:** Method of testing the plan by distributing copies to each of the functional areas. Each area reviews the plan and checks off the points that are listed. This process ensures that the plan addresses all concerns and activities.
- **Tabletop Exercise:** Participants review and discuss the actions they would take per their plans, but do not perform any of these actions. The exercise is typically under the guidance of exercise facilitators.

- **Standalone Test:** A test conducted on a specific component of a plan, in isolation from other components, typically under simulated operating conditions.
- **Integrated Test:** A test conducted on multiple components of a plan, in conjunction with each other, typically under simulated operating conditions
- **Simulation Test:** Where all operational and support functions meet to practice execution of the plan based on a scenario that is played out to test the reaction of all functions to various situations. Only those materials and information available in a real disaster are allowed to be used during the simulation, and the simulation continues up to the point of actual relocation to the alternate site and shipment of replacement equipment. (a.k.a. Scenario Testing)
- **Parallel Test:** Essentially an operational test. In this test, the critical systems are placed into operation at the alternative site to see if things run as expected. The results can be compared with the real operational output and differences noted
- **Full Interruption Test:** When full normal operations are completely shut down, and the processing is conducted at the alternate site using the materials that are available in the offsite storage location and personnel that are assigned to the recovery teams.

When to Update Plan:

- Business Unit changes
- Business Strategy changes
- Business Process changes
- IT System changes

Enterprise Architecture:

Terms & Definitions:
RAM: Random Access Memory (volatile)
ROM: Read Only Memory (nonvolatile)
CPU: Brain. Fetches instructions from memory and processes them
Registers: Temporary storage location (fastest portion of CPU cache. Fastest form of memory)
Control Unit: Manages jobs
ALU: Arithmetic Logic Unit. Performs math calculations. Fed by control unit.
Address Bus: Primary communication channel. Requests
Data Bus: Returns
System Unit: Computer's case and everything within it
Pipelining: combining multiple steps into one combined process
Stack: In Memory, per process
Process: Collection of instructions and assigned resources. Communicate between rings w/system calls
PSW- Program Status Word: Conditions are User/Privileged Mode
Multiprocessing: Having more than one CPU. Symmetric=load balancing Asymmetric=dedicated to app
Multiprogramming: Multiple programs running simultaneously on one CPU
Multitasking, **Cooperative**: Multiple processes running on one CPU. Relies on application
Multitasking, **Preemptive**: Multiple processes running on one CPU. Controlled by OS
Multithreading: Application can run multiple threads simultaneously
Watchdog Timer: Recovers a system by rebooting after a critical process hangs or crashes

Layering: Separates hardware and software functionality into modular tiers (hardware, kernel, OS, app)
Abstraction: Hides unnecessary details from the user
Security Domain: List of objects a subject is allowed to access (groups of subjects & objects with similar security requirements). Examples: Confidential, Secret, Top Secret
Open System: Uses standard components from different vendors, based on standards
Closed System: Uses proprietary hardware or software

TSEC (Orange Book): Trusted computer system evaluation criteria
TCB (Trusted Computing Base): Security-relevant portions of a computer system
Security Perimeter: Divides what is in TCB from what isn't
Reference Monitor: Mediates access between subjects and objects (enforces security policy on MAC)
Security Kernel: Access Control component of TSB. Enforces reference monitor rules
State Transition: An activity that alters the state of a system

ITSEC/ITSEM: Analysis of assets, threats, risks, confidence, and countermeasures. Replaced by CC
Common Criteria: International standard for security evaluation criteria for information processing syst

Certification: An assessment, or technical review of a product to ensure security requirements are met
Accreditation: Management (data owner) acceptance of the certification & decision (assume/mitigate)

Process States:
- **New**- Process being created
- **Ready**- Waiting for a request from a user
- **Running**- Instructions currently being executed by CPU
- **Stopped**- Not running
- **Waiting**- Waiting for an interrupt for further processing
- **Terminate**- Completed a process

System Self-Protection:
- Levels of access to resources and trust levels (Rings 0-3) (higher trust = more capabilities)
- **Memory segmenting/protection**: Prevents one process from affecting another

- **Process isolation:** logical control to prevent one process from interfering with another
- **Layering and data hiding** (low-level processes can't communicate directly to higher-level)
- **Virtual machines**
- **Protection rings**
- **Security domains**
- **Trusted Computing Base**

Protection rings

- CPU/Hardware layering forming barriers between components of different trust levels
  - Ring 0: Kernel (the interface between hardware and the rest of the OS)
  - Ring 1: OS components not in ring 0
  - Ring 2: Device Drivers
  - Ring 3: User Applications
- Requires them to communicate through strict interfaces
- When processes execute, they do so in a security context – user/privileged mode – depending upon Ring
- Processes can access resources in same or LOWER ring only
- Processes with higher trust level have larger domain of system resources available

Trusted Computing Base (TCB):

- Security portions of a computer system (all mechanisms providing protection for a system)
- Trusted processes execute in privileged mode
- Security Perimeter divides what is in TCB from what isn't

Security Models:

- **The Bell-LaPadula Model:**
  - Objective= Confidentiality (does NOT address integrity) [Military/Government]
  - Focus= Security Levels
  - (MAC) Mandatory Access Control
  - Mathematical model describing access control
  - Subjects, Objects, and Access Control Matrix
  - Properties:
    - Simple Security Property (ss-property): NO Read Up
    - * Property: No Write Down
    - Strong Tranquility Property: sec. labels won't change while system is operating
    - Weak Tranquility Property: sec. label changes won't cause security conflicts
- **The Biba (Integrity) Model:**
  - Objective = Integrity (does NOT address confidentiality) [Private Businesses]
  - Focus= Integrity Levels
  - (MAC) Mandatory Access Control
  - Higher integrity level = more confidence in reliability and accuracy
  - Properties:
    - Simple Integrity Property (SI-Property): NO Read Down
    - Integrity * Property: NO Write Up
- **The Brewer and Nash Model (Chinese Wall):**
  - Objective= Address conflicts of interest by dynamically denying access based on previous access (1 company servicing both Coke and Pepsi. A user accessing either is subsequently denied access to the other)
  - Mathematical theory to implement dynamic access permissions
- **The Clark-Wilson Model:**
  - Objective = Integrity
  - Requires subjects to access objects via programs. Requires that users are authorized to access and modify data, and that data is only modified in authorized ways
  - Enforces separation of duties and transformations procedures within systems
  - Access control triple: User, Transformation Procedure, and Constrained data item
    - Transformation Procedure(TP): A well-formed transaction
    - Constrained data item (CDI): The data requiring integrity

- **The Lattice Model:** Defines upper and lower access limits. Access is evaluated based on: subject need, object label & subject role. Uses Least Upper Bound & Greatest Lower Bound
- **State Machine Models:**
  - Groups all possible system occurrences, called states & evaluates possible interractions
  - Assumes complete knowledge of states, actors & transitions. Once change= restart
- **Access Matrix Model:**
  - A table defining what access permission exists between subjects and objects. State machine model for a discretionary access control environment
- **The Information Flow Model:**
  - Defines how information may flow in a secure system. Simplifies analysis of covert channels
  - Used by both Bell-LaPadula and Biba
- **The Noninterference Model:**
  - Ensures data at different security domains remain separate from one another
  - Prevents subjects in one domain from affecting each other in violation of security policy
- **The Graham-Denning Model:** Granular approach for interaction between subjects & objects. Has eight rules
- **The Harrison-Ruzzo-Ulman Model:** Variation of Graham-Denning. Uses an access matrix

Modes of Operation:

- **Dedicated:** System contains objects of 1 classification level only
- **System High:** System contains objects of missed classification levels. Subjects require clearance equal to highest object classification level in the system
- **Compartmented:** uses technical controls to enforce need to know on the system
- **Multilevel:** Uses reference monitor to mediate access between subjects and objects

TCSEC (Orange Book) Ratings: (A1 is best. Higher levels meet all lower level requirements too)

- **A1:** Verified Design
- **A: Verified Protection (formal methods)**
- **B3:** Security Domain
- **B2:** Structured Protection
- **B1:** Labeled Security Protection
- **B: Mandatory Protection (MAC)**
- **C2:** Controlled Access Protection
- **C1:** Controlled Security Protection
- **C: Discretionary Protection (DAC)**
- **D: Minimal Security**

TNI (Red Book): TCSEC concepts applied to Network Systems

ITSEC (European IT Security Evaluation Criteria):

- **International**: First successful international evaluation model.
- Separates Functionality (how well it works) from Assurance (effectiveness & correctiveness)
- ITSEC Assurance Ratings & their equivalent in TCSEC:
  - E0: D1
  - F-C1,E1: C1
  - F-C2,E2: B1
  - F-B2,E4: B2
  - F-B3,E5: B3
  - F-B3,E6: A1

International Common Criteria:

An internationally agreed upon standard for describing and testing the security of IT products
Answers what security mechanisms are in place and how reliable they are
Combines the strengths of TSEC and ITSEC while eliminating the weaknesses. Globally recognized.

- **Terms:**
  - **Protection Profile (PP):** General security requirements & objectives for similar products
  - **Target of Evaluation (ToE):** Product proposed to provide security solution
  - **Security Environment:** Laws, security policies, threats, etc. where the ToE will be used
  - **Security Objectives:** How policies, assumptions & threats will be satisfied/countered
  - **Security Target (ST):** Security objectives & requirements for a specific ToE
  - **Packages (Evaluation Assurance Levels (EAL)):** Functional & assurance requirements are bundled into packages for re-use. Describes what must be met to achieve a EAL.
  - **ToE Security Requirements:** Technical requirements for security functions & assurance
  - **ToE Security Specifications:** Defines proposed implementation of the ToE
  - **ToE Implementation:** Realization of ToE in accordance with specification

- **EAL: Evaluation Assurance Levels:** (certification under the common criteria)
  - **EAL1 -** functionally tested
  - **EAL2 -** structurally tested
  - **EAL3 -** methodically tested and checked
  - **EAL4 -** methodically designed, tested and reviewed
  - **EAL5 -** semiformally designed and tested
  - **EAL6 -** semiformally verified design and tested
  - **EAL7 -** formally verified design and tested

Security Architecture:

- Mission: Protect & secure intellectual property
- Provides a framework for managing intellectual property **(AAA & CIA)**

Component Security Analysis:

- **Assurance**: Documentation, Certification level, Physical security
- **Accountability**: Identification / AAA, Logging (detail, analysis & alerting tools/automation level)
- **Accuracy**: Integrity checking mechanisms (batch and hashing totals, crypto hash, checksum)
- **Access Control**: Discretionary Access Control, Secure system startup, least privilege, segregation of duties, group policy mgmt
- **Secure data exchange / communications:** Network Peer entity authentication, Network Data integrity, Network Data confidentiality, Non repudiation of origin / receipt, Network Access control.
- **Availability**: Backup and restore, Prevention of Resource Abuse, Change/release management, Redundancy / Replication, Disaster Recovery
- **Object Reuse Model**

Database Security:

Polyinstantiation: Two objects have same name (primary key), but different labels & data
Inference and Aggregation: Using lower level access to learn restricted information
Data Mining: Searching large amounts of data to find patterns that would otherwise be lost in volume

Countermeasures: Controls put into place to mitigate risk (Defense in depth)

- **Technical**: Firewalls, NIDS, HIDS, etc.
- **Administrative**: Policies, Procedures, Guidelines, Standards, etc.
- **Physical**: Security Guards, Locks, etc.

Threats to Systems:

- **Backdoor**: Shortcut in a system allowing an attacker to bypass security checks
- **Maintenance Hook**: Backdoor implemented for debugging during development. Allows direct access to code and command execution outside standard access control model

- **TOC/TOU (Time-of-check/time-of-use attack):** Race Conditions: Attacker alters a condition after it has been checked by the OS, but before it is used.
- **Asynchronous Attack (Race Condition):** Takes advantage of serial execution of instructions by making a process execute out of sequence (ex. forcing authorization before authentication)
- **Buffer Overflow**: Too much data accepted as input into a process. Result= command execution. Occurs when a programmer fails to enforce bounds checking.
- **SQL Injection**: Injecting SQL code into the database without passing through the application
- **SYN Flood**:
- **Session Hijacking:**
- **Man-in-the-Middle (MITM):**
- **DDoS:** Distributed denial of service attack (flooding system or application to make unavailable)
- **Cold Boot Attack:** Unplugging a system, then quickly booting off DVD or USB and performing a memory dump, in order to obtain what was in RAM (i.e. encryption keys in plain text)
- **Emanations:** Energy escaping an electronic system, which can be monitored
- **Covert Channels:** Any communication violating security policy
- **Covert Storage Channel:** Using shared storage for two subjects to communicate restricted info
- **Covert Timing Channel:** Using system clock to infer sensitive information, such as a login error being more quickly returned when a bad username is entered than when a good user bad pass.
- **Server-Side Attacks:** Launched from an attacker to a service to exploit vulnerabilities in services
- **Client-Side Attacks:** User downloads malicious content from an attacker
- **Malware:**
    - **Viruses:** Malware that doesn't spread automatically. Requires a carrier
    - **Worms:** Self-propagating malware
    - **Trojans:** Malware hidden in a functional application
    - **Rootkit:** Malware that replaces portions of the kernel and/or OS (Ring 3)
    - **Packers:** Provide runtime compression of executables to evade AV signatures
    - **Logic Bomb:** Malicious program triggered when a pre-defined condition is met

Web:

- **XML**: A standard way to encode documents & data. Users can define their own data format
- **SAML**: XML-based framework for exchanging security information. Used in single sign-on.
- **Applets:** Small pieces of mobile executable code embedded in other software, such as web browsers. Mostly written in Java (called 'applets'), and ActiveX (called 'controls').
- **Java:** Object-oriented, platform-independent language. Interpreted by the JVM.
    - **Sandboxing:** Java applets run in a sandbox, which segregates the code from the OS
- **ActiveX:** Like Java applets, but they use digital certificates to provide security (not a sandbox)

Mobile Security:

- **Administrative Control:** Mobile Device Policy restricting the use of mobile devices (smartphones, USB drives, Laptops, etc.)
- **Technical Control**: Require authentication at layer 2 through:
    - **NAC (802.1x)**: Network device-based solution supported by several vendors
    - **NAP:** Computer OS-based solution supported by Microsoft

PCI-DSS:

Core Principles:

- Build & maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Access Control:

Terms & Definitions:
Subject: Active entity on an information system (either people or applications) accessing resources
Object: Passive entity/resource (ex. database, text file)
(DAC) Discretionary Access Control: Subjects have full control of objects they are given access to
(MAC) Mandatory Access Control: System-enforced access control based on subject's clearance & object's label
(RBAC) Role-Based Access Control: Subjects grouped into roles and permissions are defined by a particular role
Confidentiality Levels: Also called Security Domains (ex. Confidential, Secret, Top Secret)
Data Owner: Determine information classification level, and determine who may access the data
Data Custodian: Guardian of the data, appointed by Data Owner. Perform backups, maintain access lists, etc.
User: Entity accessing the data
Least Privilege: (Preventive) Limits a user's access to the minimal amount required to do their jobs
Separation of Duties: (Preventive) Critical/Sensitive transactions broken up across more than one person
Rotation of Duties / Mandatory Vacation: (Detective) Required different people perform same duty
Collusion: Two or more people conspire to subvert the security of a system
Need to Know: More granular than least privilege. Subject's need to know is evaluated for each individual object
(ACLs) Access Control Lists: A list of objects, each entry listing the subjects authorized to access that object
Credential Set: The combination of both Identification and Authentication of a user

Access Control Basics:
- **Purpose:** Allow authorized users access to appropriate data & deny access to unauthorized users
- **Mission:** To protect the Confidentiality, Integrity, and Availability of data
- **Method:** Implement Administrative, Physical, and Technical (Logical) controls

(CIA) Information Security Triad:
Goal: To balance the needs of the three, making trade-offs when necessary
- **Confidentiality**: Prevents unauthorized read access to data (prevents unauthorized disclosure of info)
- **Integrity**: Prevents unauthorized write access to data (prevents unauthorized modification of info)
- **Availability**: Ensures information is available when needed

(AAA) Identity and Authentication, Authorization, and Accountabilty:
- **Identity**: An identity claim is someone stating who they are (ex. User Name) [NO Proof]
  - Identities must be unique, and must only be used by one user
- **Authentication**: Proving an identity claim by supplying secret information (ex. Password)
  - Two-factor / multi-factor / strong authentication are preferred
- **Authorization**: The actions permitted once Identification & Authorization take place (Permissions)
  - Authorization Creep: When subjects move to new roles, retain old access & get new access
- **Accountability**: Holds users accountable for their actions, typically through logging & monitoring
- **Non-Repudiation:** User is not able to deny. Logs transactions by users & ensures integrity of the logs

Passwords:
- Weakest, Cheapest, Most popular form of access control
- **Weaknesses:** Insecure, Easily broken, Inconvenient, Repudiable
- **Attacks**: Sniffing, Social Engineering, Accessing password file/db, Dictionary attack, Brute force, etc.
- **Safeguards/Controls:** Account lockout, Password hashing, Password aging
- **Password Types:**
  - **Static Passwords:**
    - User uses same password each time
  - **Synchronous Token Device:**
    - Token generates new unique password value at fixed time interval
  - **Asynchronous Token Device:**
    - Token generates new unique password asynchronously (not on a timing interval)

- **Memory Card:**
  - Magnetic stripe, relies on a reader and processes externally
- **Smart Card:**
  - Contains a computer chip, relies on a reader, and can process internally

Access Control Models:

One model is not inherently better/worse. Each model is used for a specific information security purpose

- **(DAC) Discretionary Access Control:**
  - ACLs are used to enforce security policy
  - Subjects have full control of objects they've been given access to
  - Subjects can grant other subjects access to their files, change file attributes, delete files, etc.
  - Examples: Windows, Linux and Unix file systems
  - Mistakes and malicious acts can result in loss of Confidentiality, Ingegrity, or Availability
- **(MAC) Mandatory Access Control:**
  - System-enforced access control based on subjects' clearance and object's label (classification)
  - Subjects can only access objects if their clearance is greater than or equal to the object's label
  - Focuses on Confidentiality. The Bell-LaPadula security model is based on MAC
  - Examples: (LIDS) Linux Intrusion Detection System, SCOMP, and Purple Penelope
  - MAC is expensive and difficult to implement
- **Non-Discretionary Access Control:**
  - Subjects don't have discretion regarding groups of objects they access, and can't transfer objects
  - **RBAC Role-Based Access Control**
    - Defines how data is accessed on a system based on the role of the subject
    - Subjects are grouped into roles and permissions are defined based on a particular role
    - **Rules:**
      - **Role Assignment:** Subject can execute a transaction only if it has been assigned a role
      - **Role Authorization**: A subject can only take on roles for which they are authorized
      - **Transaction Authorization:** Transaction must be authorized through subject's role
  - **(TBAC) Task-Based Access Control:**
    - Access control based on tasks each subject must perform

Access Control Methods:

- **Capability Tables:** Based on Subjects. (User x has access to objects 1, 2, 3, 4, etc.)
- **(ACLs) Access Control List/Matrix:** Based on Objects. (Users x, y & z have access to object 1)
- **Restricted/Constrained User Interfaces:** Limits user's environment within the system
- **Database Views:** Presents a subset of data in the database to users (certain rows & columns)

Content and Context-Dependent Access Controls:

Not full access control models, but play a defense-in-depth supporting role. Typically implemented with DAC

- **Content-Dependent Access Control:**
  - Adds criteria beyond identification & authorization: the content the subject is attempting to access
  - Example: Granting access to the HR database, but only for that particular user's record
- **Context-Dependent Access Control:**
  - Applies additional context before granting access to subjects
  - Example: Time is a context that can be used to deny login attempts after working hours

Centralized and Decentralized/Distributed Access Control:

- **Centralized Access Control:**
  - Concentrates access control in one point, rather than using many local access control databases
  - Example: (SSO) Single Sign-On- Subject authenticates once then may access many systems
- **Decentralized/Distributed Access Control:**
  - Provides local control to employ different access control models, policies, and levels of security
  - Often used when an organization spans multiple sites

Authentication Protocols:

- **(PAP) Password Authentication Protocol:**
  - Weak authentication method designed for use with PPP
  - 2-way handshake protocol where passwords sent in plaintext
- **(CHAP) Challenge Handshake Authentication Protocol:**
  - 3-way handshake protocol. Central authentication location stores a secret (no playback attacks)
  - Authentication is one-way, but one can be negotiated in both directions
- **(EAP) Extensible Authentication Protocol:**
  - Most Secure. Determines what authentication protocol will be used. Allows many options

Authentication Technologies:

- **Single Sign-On:**
  - Multiple systems to use a central authentication server (AS). Authenticate once & access many
  - **Pros:** , simplifies user provisioning & deprovisioning, simplifies user permission changs, and Improves productivity of users (1 pass to remember), developers (auth framework), and admins
  - **Cons:** Difficult to retrofit, creates a single point of attack, and makes credential disclosure worse
  - **Single Sign-on Technologies:**
    - **Kerberos:**
      - **S**ymmetric keys (called Tickets)
      - Stateless (Issued credentials are good for the credential lifetime)
      - A network authentication system for use on insecure networks
      - Provides mutual authentication of client and server
      - Allows entities to prove identity
      - Prevents eavesdropping & replay attacks
      - Rogue KDCs won't work, because they won't have access to real keys
      - All system clocks participating in Kerberos must be synchronized
      - KDC stores plaintext keys of all Principals, so it's a single point of attack
      - KDC and TGS are single points of failure (no new credentials issued if down)
      - **Kerberos Components:**
        - **Principal**: Client (user), or service
        - **Realm**: A logical Kerberos network
        - **Ticket**: Data that authenticates a principal's identity
        - **Credentials**: A ticket and the service key
        - **(KDC) Key Distribution Center:** Authenticates principals
        - **(TGS) Ticket Granting Service**
        - **(TGT) Ticket Granting Ticket**
        - **(C/S) Client Server**: Communication between the two
      - **Kerberos Steps:**
        - Principal (user) contacts KDC, requesting authentication
        - KDC sends: session key encrypted with Principal's secret key, and a TGT encrypted with TGS's secret key, to the Principal
        - Principal decrypts their session key & requests resources through TGS
        - TGS validates TGT key & sends C/S session key and a Service Ticket to the Principal, encrypted with the desired resource's secret key
        - Principal connects to desired resource, which validates the Service Ticket and C/S key
        - ****NOTE**** User can't decrypt TGT, only the TGS can
    - **SESAME (Secure European System for Applications in Multi-vendor Environment)**
      - Sort of a sequel to Kerberos
      - Adds Asymmetric encryption, to prevent plaintext storage of symmetric keys
      - Uses (PACs) Privilege Attribute Certificates in place of Kerberos tickets

        - Adds heterogeneity, scalability, better manageability, and better auditing
    - **SAML:** Identity assertions using web services

Network-Level Authentication:

- **(RADIUS) Remote Authenticaiton Dial In User Service:**
    - Provides: AAA- Authentication, Authorization & Accounting
        - Authenticates subject's credentials against an authentication database
        - Authorizes specific subjects access to specific objects
        - Accounts for each session by creating log entries for each connection made
    - Request & Response data is carried in (AVPs) Attribute Value Pairs (8-bits) (256 possible AVPs)
    - Weaknesses: Limited accountability, flexibility, scalability, reliability, and security
    - Requires many servers (one server per connection protocol)
    - Only encrypts password. Username is left unencrytped
- **Diameter:**
    - Successor to RADIUS, providing improved AAA
    - More flexible, scalable, reliable, and secure than RADIUS
    - Request & Response data is carried in (AVPs) Attribute Value Pairs (32-bits) (billions possible)
    - Uses a single server to manage policies for many services (one server for unlimited protocols)
- **(TACACS) Terminal Access Controller Access Control System:**
    - Centralized Access Control (Cisco proprietary) [Uses TCP]
    - Users send an ID and a static (reusable) password for authentication
    - Ports: UDP or TCP: 49
- **(TACACS+)**
    - Improves on TACACS (Cisco proprietary) [Uses TCP]
    - Permits two-factor / multi-factor / strong authentication
    - Not backward-compatible with TACACS
    - Encrypts all data below the TACACS+ header (usernames, passwords, data, etc.)
- **Microsoft Active Directory Domains & Trusts:**
    - In Windows, domains are the primary means to control access
    - Windows trust relationships are authenticated using Kerberos (separate process/domain)
    - One-way trusts: Trusted domain users can access Trusting domain resources
    - Transitive Trusts: Trust extends to Trusted's Trusted | NonTransitive: Only explicitly set trusts

Access Control Defensive Categories & Types:

- **Access Control Types:**
    - **Preventive:** Prevents harmful occurrences by restricting what a potential user can do
        - Physical: Lock, Mantrap | Technical: Firewall | Admin: Pre-employment drug screen
    - **Detective:** Controls that alert during or after a successful attack (ex. IDS/IPS, CCTV, Alarm)
        - Phsyical: CCTV, Light | Technical: IDS | Admin: Post-employment random drug screen
    - **Corrective:** Restores systems that are victims of harmful attacks (often bundled with Detective)
    - **Deterrent:** Discouraging unwanted actions (ex. Beware of Dog sign, documented punishment)
        - Physical: Beware of Dog sign | Administrative: Sanction policy
    - **Recovery:** Restore functionality of the system and organization (ex. re-image a PC, Restore, etc.)
    - **Compensating:** Compensate for weaknesses in other controls (ex. reviewing users web usage)
    - ***Look for context to determine the control Type. Questions will often have context***
- **Access Control Categories:**
    - **Administrative (Directive):** Prohibiting through: Policies, procedures, security awareness, etc.
    - **Technical (Logical):** Restricting using technology (ex. encryption, ACLs, Network segmentation
    - **Physical:** Restricting physical access using physical objects (ex. guards, locks)

Labels/Classification, Clearance, Formal Access Approval, and Need to Know:

- **Labels:** Security classifications (Confidential, Secret, Top Secret) applied to objects
- **Compartments:** Require a documented & approved need to know, in addition to the label's clearance
- **Clearance:** A determination of a Subject's current and potential future trustworthiness (Top Secret, etc.)
- **Formal Access Approval:** Documented approval from Data Owner for a subject to have access to object

Authentication Types / Methods:

- **Type I:** Something you Know (ex. static password) Tested via a challenge and response
- **Type II:** Something you Have (ex. secure token, credit card, ATM card, smart card, etc.)
- **Type III:** Something you Are (ex. biometrics)
- **Type IV:** Some place you are (location-based). (ex. GPS, IP Address, Geo-location)

Passwords:

Cheapest, Weakest, Most Popular form of authentication (Type I)

- **Type s of Passwords:**
  - **Static Password:** Reusable, typically user-generated passwords. May or may not expire
  - **Passphrase:** a long Static password comprised of several words in a sentence, with punctuation
  - **Dynamic Password:** Change at regular intervals (ex. Synchronous secure tokens (ex. SecureID))
  - **One-Time Password:** Used for a single authentication. Difficult to manage
  - **Strong Authentication:** Two-factor, Multi-factor authentication. Combines two+ Types
- **Password Hashes:**
  - Hashed values of passwords should be stored in IT systems instead of plaintext passwords
  - **Hashing:** One-way encryption using an algorithm and no key
  - **Salt:** Random character(s) added to a passwords to allow one password to hash multiple ways. Each password must be hashed with each possible salt value in order to be successful
  - **Password Storage:**
    - Unix/Linux stores passwords in: /etc/shadow (readably only by Root user)
    - Windows stores passwords in: SAM File (both locally and on the domain controller)
  - Password hashes can be sniffed on the network, or dumped from memory
  - Law enforcement Investigations:
    - Hashes the entire hard drive first (used to verify integrity of evidence in court)
    - Performs a binary (bit-by-bit) copy of the drive & works off that copy
- **Password Attacks:**
  - **Dictionary Attack:** Use a list of predefined words then run each through a hashing algorithm
  - **Brute-Force Attack:** Calculate the hash value of every possible password, then try one-by-one
  - **Rainbow Table:** A database containing pre-computed hash values for most possible passwords
  - **Hybrid Attack:** Appends, prepends, or changes characters in a dictionary attack before hashing. Used to determine passwords where people use numeric substitution for letters or add a "!" at end
- **Password Management:**
  - Enforcing: Password history, Minimum age, Maximum age, Complexity requirements, etc.

Dynamic Tokens:

- **Synchronous:** Use time or counters to synchronize token code with the server (ex. RSA SecureID)
- **Asynchronous:** User responds to challenge with response + PIN (ex. Smart Card)

Biometrics:

- **Uses:** Establish an identity (ex. facial recognition) or to Authenticate (ex. fingerprint scan)
- **Acceptable Enrollment Time:** 2 minutes
- **Acceptable Throughput Rate:** 6-10 subjects/minute (6-10 seconds/subject)
- **Pros:** Easier for employees to manage, reliable, resistant to counterfeiting, small data storage requirement
- **Cons:** Can cause privacy issues,
- **Errors:**
  - **Type I Error (FRR): %** Falsely Rejected (Deny Authorized user)
  - **Type II Error (FAR):** % Falsely Accepted (Permit Intruder)
    - **Two is greater than One:** Rule to remember Type II errors are worse than Type I
  - **(CER) Crossover Error Rate:** Where % of Type 1 errors = % of Type 2 errors. (Low = good)
- **Order of Effectiveness**
  - **Iris scan:** Passive control. Camera takes picture of the colored portion of the eye
  - **Retina scan:** (Intrusive) Laser scans capillaries in back of eye. Retina changes due to health

  - **Fingerprint**: Most widely used (ex. smart cards, smart keyboards). Whorls, ridges, bifrucations
  - **Hand geometry**: Measures specific points on subject's hand (length, width, thickness) ~9 bytes
  - **Voice pattern:** Measures tone of voice for certain words/sentences. Vulnerable to replay attacks
  - **Keystroke Dynamics:** The rhythm and force a person uses when entering a password
  - **Dynamic Signature:** Measures time, pressure, loops, begin/end points of a person's signature
- **Order of Acceptance**
  - Voice Pattern
  - Keystroke Dynamics:
  - Dynamic Signature
  - Hand geometry
  - Fingerprint
  - Iris scan
  - Retina scan

(IDS) Intrusion Detection System:

- Monitors network traffic or monitors host audit logs to determine if security policy violations exist
- Can detect intrusions that have passed through a firewall or are occurring inside the firewall
- **Types:**
  - **(NIDS) Network-Based IDS:**
    - Captures and analyzes network packets
    - Runs in Promiscuous Mode to monitor all traffic (not just traffic for its MAC address)
    - **Advantages**: Few boxes cover large surface area | Little impact on network
    - **Disadvantages**: Blind to encrypted data | May not scale | Doesn't like segmentation
  - **(HIDS) Host-Based IDS:**
    - Collects information from an individual machine
    - **Advantages**: Detects application level attacks | Can decrypt | Unaffected by switches
    - **Disadvantages**: Highly distributed | Consume host resources | OS can suffer a DoS
- **Methods:**
  - **Signature Based:**
    - Pattern matching, so must be known by product
    - Must be frequently updated, and fails against new attacks
  - **Statistical Anomaly Based:**
    - Behavior-based. Learns "normal" activities
    - Can detect new attacks
  - **Protocol Anomaly Based:**
  - **Traffic Anomaly Based:**
  - **Rule-Based:**
    - Uses an Expert System (If/Then statements)
    - **Types:**
      - **State Based**: Tracking system state changes to identify attacks
      - **Model Based:** Models of attack scenarios are built & used for comparison

Types of Attackers:

- **Hacker:** Can be black hat (bad guys) or white hat (good guys)
  - A person who enjoys learning details of systems & stretching their abilities
- **Cracker**: A malicious Hacker (aka Black Hat)
  - A person who cracks software copy protection, or a person who cracks password hashes
- **Script Kiddies:** People who attack systems using tools they have little or not understanding of
- **White Hat:** Good guys who have authorization to hack (ex. Penetration testers)
- **Gray Hat:** A person who exploits a security weakness in a system to bring alert the owner of the weakness
- **Hacktivist:** Hacker activist. Attacks systems for political reasons
- **Phisher:** Malicious attacker using social engineering to trick users into divulging credentials or PII

Methods of Attack:

- **Port Scans**
  - Information gathering. Typically one of the first steps in attacking a site.
- **Social Engineering**
  - Confidentiality/Integrity attack: leveraging nice people to gain unauthorized access
- **Buffer Overflows**
  - Confidentiality/Integrity/Availability attack: exploiting software bugs to write malicious code
- **Denial of Service**
  - **Availability attack:** diminish or disrupt systems or services
  - **Syn Flood –** TCP handshake vulnerability
  - **Ping of Death –** Large ICMP packets
  - **Teardrop –** IP fragmentation DOS
  - **Smurf -** Spoofed ICMP to broadcast addresses
  - **Fraggle -** Spoofed UDP to broadcast addresses
- **(DDoS) Distributed Denial of Service**
  - Availability attack using zombie machines, large scale worm, or virus
- **Backdoor**
  - Confidentiality/Integrity/Availability attack: Undocumented, non-standard access to a system
- **Trojan Horse (RAT: Remote Access Trojans)**
  - Confidentiality/Integrity/Availability attack: Integrity/Confidentiality/Availability attack: Legitimate applications that contain malicious code
- **Brute Force**
  - Integrity/Confidentiality attack: Sequential run-through of all possible password combinations
- **Dictionary Attack**
  - Integrity/Confidentiality attack: Run through well-known words with various rules to try and guess passwords
- **Spoofing**
  - Integrity/Confidentiality attack: Acting as someone else
- **Man-In the Middle**
  - Confidentiality/Integrity attack: Spoof identity of client and server to intercept traffic
- **Spamming**
  - Confidentiality/Integrity attack: Unauthorized bulk email
- **Sniffing**
  - Confidentiality attack: Watching network traffic

Security Audit Logs:

- **Common Log Management Problems**
  - Not regularly reviewed
  - Not stored long enough
  - Not standardized or able to be correlated
  - Not prioritized
  - Logs are only reviewed for a handful of bad things
- **Logs to Collect:**
  - **Network Security Software/Hardware:**
    - Antivirus logs
    - IDS/IPS logs
    - Remote access software (ex. VPN logs)
    - Web Proxy
    - Vulnerability management
    - Authentication servers
    - Routers and firewalls
  - **Operating System:**
    - System events
    - Audit records
  - **Applications:**

- Client requests and server responses
- Usage information
- Significant operational actions

Network & Telecommunications Security:

Terms and Definitions:
OSI Model: 7-layer network model created by the ISO (App, Pres, Sess, Tran, Net, DL, Phys)
TCP/IP Model: 4-layer network model (Network access, Internet, Transport, Application)
Packet-Switched Network: Shared Bandwidth | data carried in packets
Circuit-Switched Network: Dedicated Bandwidth (old voice circuits, T1, etc.)
Port: A specific point of entry and departure point for network traffic to an application
1024 well known ports | 65,535 total ports |
Socket: A combination of source and destination IP address and source and destination port
Message: Data to be transmitted
Segment: Data after processing by TCP at Transport layer
Datagram: Data after processing in Network layer (routing and addressing info added)
Frame: Data after processing in Data Link layer (header & trailer added)
Packets: Generic term to describe data moving through the network at any stage
Subnet: Breaking a network segment into smaller increments for better control & management
Classful: Use of traditional subnet masks | Classless: Use of non-traditional subnet masks
Asynchronous Transmission: No device synchronization. Use a "Stop Bit" to end a transmission
Synchronous Transmission: Devices are synchronized. Uses a "Clock Signal" to end a transmission

OSI Model:

- Open network model allowing disparate Open Systems & networks to communicate
- Traffic flows Application to Physical for sender, Physical to Application for receiver
- Each layer adds information to the traffic (encapsulation) on sending & removes on receiving

Layer	Name	Protocols	Description
7	Application	HTTP SMTP FTP TFTP Telnet	Where users interface with computer applications. Provides specific services for applications such as file transfer, instant messaging, etc.
6	Presentation	JPEG GIF TIFF	Presents data to the application & user in a comprehensible way. Data encryption and compression happen here. ASCII characters & image formats live here.
5	Session	NFS SQL NetBIOS RPC	Establishes, maintains & manages connections (sessions) between Applications. [Modes: Simplex, Half-Duplex, Full-Duplex]. RPCs live here.
4	Transport	TCP UDP SPX	Manages connections (sessions) between Systems. Connection-oriented. Uses a handshake process. Handles packet sequencing, flow control, and error correction (TCP). UDP doesn't implement many of these
3	Network	IP ICMP OSPF BGP RIP IGMP	Addresses, switches, and routes network packets. Moves data from one system on one LAN to a system on another LAN. Does Not ensure delivery.
2	Data Link	PPP SLIP RARP L2TP L2F FDDI	Determines the format the data frame must be in (Ethernet, Token Ring, FDDI, etc.) Provides transfer of units of information to other end of physical link. NICs operate here. Sub-layers: LLC: Talks up to Network (802.2) MAC: Talks to Physical (802.3, .5. .11)

		ISDN	
1	Physical	HSSI X.21 EIA/TIA	Converts bits into energy (voltage, light, etc.), and sends them across physical medium. Controls synchronization, data rates, line noise, and media access

Devices and OSI Layers:

Computers: All 7 layers

Firewalls: Packet Filter & Stateful:= layers 3&4 | Proxy= layers 5-7 | Filter traffic between networks

- **Packet Filter:** Simple, Fast. Each packet is viewed individually for filtering decisions (no state known)
- **Stateful:** Use state table to compare current & previous packets. Slower than Packet Filter but more secure
- **Proxy:** Act as an intermediary server. Connections terminate at the proxy
  - **Application-Layer Proxy:** App layer | Must understand the protocol they are a proxy for, so one is often required for each protocol (ex. FTP, HTTP)
  - **Circuit-Level Proxy:** Session Layer | Less granular decisions than App-layer, because it doesn't understand the protocol | Can filter many protocols | Example= SOCKS

Routers: Up to Network layer | Connect different networks | Use ACLs | Use IP addresses to route | Multi-homed

Switches: Typically Data Link, but can be on layer 3 or 4 | layer2=MAC, layer3=IP, layer4=policy-based

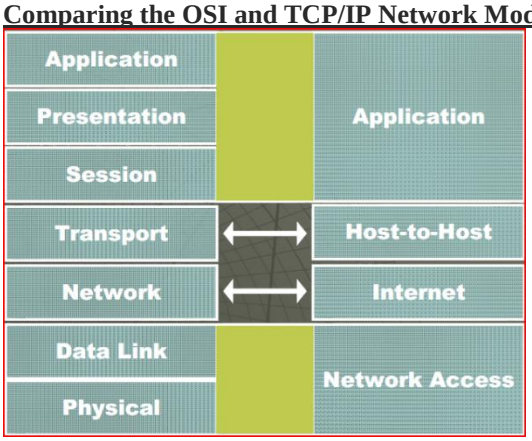
Bridges: Up to Data Link layer | Connect 2 LAN segments | Forward broadcast traffic, not collision data | MAC

Hubs: Physical layer only | multi-port repeaters/Concentrators | Uses MAC address for routing

Repeaters: Physical layer only | Amplifies Signal | Uses MAC address for routing

Sniffers (Protocol Analyzers): Sniff traffic on their LAN segment only. When bridges are used, a sniffer can see all traffic on their side of the bridge. When a switch is used, they can see only traffic on their segment to the switch.

Comparing the OSI and TCP/IP Network Models:



TCP/IP Protocol:

- Breaks information into pieces for transport through a network
- Ports 0-1023 are Reserved (well known ports) | Ports 1024-65535 are ephemeral
- Main Protocols:
  - TCP (connection-oriented): Slow, Handshaking, sequencing, flow control, error correction
  - UDP (connectionless): Fast, best delivery effort, no virtual connection. For "lossy" apps
  - ICMP: Helper protocol for troubleshooting & reporting error conditions. Uses types & codes
- TCP Handshaking Process: SYN, SYN/ACK, ACK (sets up a full-duplex connection)

IPv4 Network Classes (classful subnets):

- 32-bit address space

- Class A – Uses first byte for network (255 .0 .0 .0)
- Class B – Uses first two bytes for network (255 .255 .0 .0)
- Class C – Uses first three bytes for network (255 .255 .255 .0)
- Class D – Used for multicast addresses (255 .255 .255 .255)
- Class E – Used for research

IPv6 (IP Next Generation (IPng)):

- 64-bit address space
- Scoped addresses (multicast scalability)
- Anycast addresses added
- IPSec built in
- Auto-configuration
- No NAT needed
- QoS
- Flexible
- Vista and Windows 7 enable IPv6 by default

Dual Stack: Systems running both IPv4 and IPv6 simultaneously.
Tunneling: Hosts accessing IPv6 networks via IPv4

Network Topologies (physical layout of devices and computers):

- **Ring**: Series of devices connected by unidirectional links. A Closed loop. 1 Node failure affects network.
- **Bus**: Single cable with all nodes attached at a drop point. Cable is single point of failure
- **Star**: Central device connects all nodes. Each node has dedicated link. Central node is point of failure
- **Mesh/Full Mesh:** Internet is Mesh. All systems and resources connected to one another. High redundancy.

Types of Cabling:

- **Coaxial**: EMI resistant. Long cable runs. More expensive & more difficult to work with.
- **Twisted Pair**: Higher twists reduce EMI, increase throughput. Cheap & easy. Attn & Xtalk
  - **Cat 1**: Voice grade. Only modems for data
  - **Cat 2**: 4Mbps data
  - **Cat 3**: 10Mbps Ethernet (4Mbps Token Ring). 10BaseT installations
  - **Cat 4**: 16Mbps Token Ring
  - **Cat 5**: 100Mbps (100Base-TX and CDDI)
  - **Cat 6**: 155Mbps. Used in new network installs requiring high speeds
  - **Cat 7**: 1Gbps. Used in new network installs requiring highest speed transmissions
- **Fiber Optics:** Long distances. Expensive & hard. NO: EMI, Eavesdropping, or attenuation

LAN Technologies:

LAN Implementation	IEEE Standard	Characteristics
Ethernet	802.3	- Shared media—all devices must take turns using the same media and detect collisions. - Uses broadcast and collision domains. - Uses CSMA/CD access method. - Can use coaxial or twisted-pair media. - Transmission speeds of 10 Mbps to 1 Gbps.
Token Ring	802.5	- All devices connect to a central MAU. - Token-passing media access method. - Transmission speeds of 4–16 Mbps. - Uses an active monitor and beaconing.
FDDI	802.8	- Token-passing media access method. - Dual counter-rotating rings for fault tolerance. - Transmission speeds of 100 Mbps. - Operates over long distances at high speeds and is therefore used as a backbone. - CDDI works over UTP.

Ethernet: Layer 1 & 2. Dominant. Transmits network data via Frames. Uses Bus and Star topologies. Baseband.

Ethernet Media Access Technologies:

Type	Speed	Cable	Connector	Cable Length
10Base2 – ThinNet	10 Mbps	Coaxial	BNC	185 m
10Base5 – ThickNet	10 Mbps	Coaxial	BNC	500 m
10BaseT	10 Mbps	UTP	RJ-45	100 m
100Base-TX – Fast Ethernet	100 Mbps	UTP	RJ-45	100 m
1000Base-T – Gigabit Ethernet	1000 Mbps	UTP	RJ-45	100 m

LAN Media Access Technologies:

- **Token Passing:** 24-bit control frame. System with token can send traffic. Bit flipped on receipt
- **Collision Domains:** Systems contend for shared medium. Switches/Bridges reduce collision domains
- **CSMA:**
  - /CD: Collision Detection: Uses back-off algorithm. Transmits when available
  - /CA: Collision Avoidance: Systems send a signal before they intend to talk
- **Polling:** Systems are divided into primary & secondary. Secondary only communicate when polled

LAN Protocols:

- **ARP:** IP to MAC address mapping. Builds a table of addresses held for a while. (Masquerading)
- **DHCP:** Dynamically assigns IP addresses to systems. UDP-based. (Masqquerading, MITM)
  - **RARP:** Diskless systems broadcast their MAC address and are assigned an IP address
  - **BOOTP:** Provides diskless systems with IP address, Name server & Default gateway
- **ICMP:** Delivers status messages, reports errors, replies to some requests, fastest route to destination

Routing Protocols:

- **RIP**: Distance Vector. Legacy. Slow. V1=No auth. V2=Passwords sent in clear or MD5 hashed
- **OSPF:** Link State. More stable. Requires more CPU and Memory. Hierarchical routing
- **IGRP:** Distance Vector. Proprietary CISCO protocol. Admins set weights. Use 5 criteria for selection
- **BGP:** Link State & Distance Vector. Used by ISPs. Allows routers on different AS's to share information

Network Devices:

Device	OSI Layer	Functionality
Repeater	Physical	Amplifies the signal and extends networks.
Bridge	Data Link	Forwards packets and filters based on MAC addresses; forwards broadcast traffic, but not collision traffic.
Router	Network	Separates and connects LANs creating internetworks; routers filter based on IP addresses.
Switch	Data Link	Provides a private virtual link between communicating devices; allows for VLANs; reduces collisions; impedes network sniffing.
Gateway	Application	Connects different types of networks; performs protocol and format translations.

Firewalls: Control access from one network to another | Policies determine permitted and denied traffic

- **Packet Filtering Firewalls (Gen 1):**
  - Network Layer
  - Use ACLs to control access
  - Decisions made on header info only
  - Does NOT keep track of connection state
  - Can't control application attacks
  - Does NOT support advanced user authentication
- **Proxy Firewalls (Gen 2):**
  - Up to Application layer
  - Masks internal addresses of systems
  - Inspects traffic in both directions for harmful information
  - Can degrade performance, cause latency
  - Two Types:
    - Application-Level Proxy:
      - Look at packets up to Application layer
      - Can differentiate functions within a service or protocol (FTP Put or Get)
      - Requires a separate proxy for each service or protocol
    - Circuit-Level Proxy:
      - Session layer
      - Makes decisions based on address, port, and protocol
      - Protects link between a server and a client
      - Does NOT require a separate proxy for each communication
      - Doesn't know if traffic is safe, only knows it is between protected hosts
- **Stateful Firewalls (Gen 3):**
  - Network and Transport layers
  - Uses a State Table to track network communications
  - High security, low latency
  - Scalable and transparent
  - Vulnerably to DoS attacks
- **Dynamic Packet Filtering (Gen 4):**
  - Accepts traffic from client on "high ports"
  - Builds an ACL for the communication link so destination systems can respond
  - Can allow any traffic outbound, but only response traffic inbound
- **Kernel Proxy Firewalls (Gen 5):**
  - Creates dynamic, customized TCP/IP Stacks
  - Creates virtual stack for protocols in the packet received
  - Evaluates headers from layers 2-6

- Packet is discarded if deemed dangerous at any later
- Performs NAT services
- Faster than Application Firewalls because inspection occurs in the kernel

Firewall Best Practices:

- Explicitly deny all traffic and only allow necessary traffic
- Block inbound packets with internal addresses
- Block outbound traffic without an internal address
- Block ICMP redirect traffic
- Simple ACLs
- Disallow source routing
- Disable unused interfaces
- Close unnecessary ports
- Block directed IP broadcasts
- Block multicast traffic
- Reassemble fragmented packets before sending to higher security environments
- Enable logging

Firewall Architecture:

- **Bastion Host:** Any hardened system (all DMZ boxes should be bastion hosts)
- **Dual Homed:** Any device with 2 network interfaces for 2 networks. Disable packet forwarding
- **Screened Host:** Firewall behind router to protect private network, so router screens traffic first
- **Screened Subnet:** Two sets of firewalls set up to create a DMZ (defense in depth)

Directory Services:

- Hierarchical database of information assets, mainly for lookup operations
- Most follow X.500 Standard, and use LDAP to access the database
- Provides a resource for authentication processes
- Provides administrators with a centralized resource for system policy management
- Use schemas, like other databases

NAT: Most are stateful

- Static Mapping: Each internal device is mapped to its own external address
- Dynamic Mapping: Addresses are dynamically assigned as needed
- Port Address Translation: Only 1 external address available. Uses a port for each internal host

Metropolitan Area Networks (MAN):

- Backbone connecting multiple LANs, or LANs to WANs
- Most run on SONET or FDDI
  - FDDI:
    - Rings cover large areas
    - Networks connected via multiple technologies (ex. T1)
  - SONET:
    - Self-healing
    - Rings and lines are redundant
    - Can transmit voice, video, and data

Wide Area Networks (WAN): Backbone connecting multiple LANs, or LANs to WANs

- **Switching**
  - **Circuit Switching:**
    - Dynamically establishes virtual connection that acts as a dedicated circuit between hosts
    - All data takes the same route
  - **Packet Switching:**
    - Each packet could take a different route to the destination

        - Checks sequence numbers assigned to packets and reassembles in order
        - The Internet, x.25, and frame relay all use packet switching
- **Frame Relay:**
    - Data Link layer
    - Multiplexes multiple logical connections over a single physical connection (Virtual Circuit)
    - Focuses on speed, but has No error recovery
    - Uses packet switching
    - Multiple companies use same link
    - Charges based on bandwidth used
    - Companies can pay for a Committed Information Rate (CIR) for guaranteed level of service
    - **Frame Relay Equipment**:
        - **Data Terminal Equipment (DTE):** Customer-owned equipment attaching a LAN to it
        - **Data Circuit-Terminating Equipment (DCE):** Provider equipment doing transmission
        - **Cloud:** A collection of a series of DCE
- **Virtual Circuits:**
    - Connection-oriented
    - Used by Frame Relay and X.25
    - Two Types:
        - Permanent Virtual Circuit (PVC): For committed rate customers
        - Switched Virtual Circuit (SVC): Set up as needed, torn down after (like phone call)
- **X.25:**
    - Old switching technology where frames are addressed and forwarded
    - Any-to-any service with charged based on bandwidth used | Data divided into 128 bytes
    - Lots of error checking, error correcting, and fault tolerance
- **ATM (Asynchronous Transfer Mode):**
    - Connection-oriented
    - Uses Cell-Switching and fixed-length 53 byte cells for transmission
    - Fast and efficient
    - Reliable network throughput (all cells are 53-bytes, where Ethernet packet sizes vary)
    - Used Virtual Circuits with guaranteed bandwidth
    - Used for LAN, WAN, and MAN
- **SMDS (Switched Multimegabit Data Service)** Old technology similar to ATM (53-byte cells)
- **Quality of Service (QoS):**
    - **Constant Bit Rate (CBR):** Connection-oriented, bandwidth set by customer, for time-sensitive
    - **Variable Bit Rate (VBR):** Connection-oriented, peak and sustained rate specified by customer
    - **Unspecified Bit Rate (UBR):** Connectionless, No guaranteed performance
    - **Available Bit Rate (ABR):** Connection-oriented, left over bandwidth after guarantees are met
- **WAN Circuit Standards: (T= United States | E=Europe | DS=Any medium (not just copper)**
    - **T1:** Dedicated 1.544Mbps (24 64-bit Digital Signal o channels) | Copper phone circuit
    - **T3:** Dedicated 44.736Mbps (28 bundled T1s) | Copper phone circuit
    - **E1:** Dedicated 2.048Mbps (30 channels) | Copper phone circuit
    - **E3:** Dedicated 34.368Mbps (16 bundled E1s) | Copper phone circuit

Virtual Private Network (VPN): Secure private connection through public network

- **IPsec:** Provides CIA via encryption. Includes ESP (Encapsulating Security Protocol) and AH (Auth Hdr)
- **SSL and TLS:** Protects HTTP and other protocols | TLS is SSL version 3.1 | Easier to firewall than IPSec
- **Encapsulation Protocols:**
    - **Point-to-Point Protocol (PPP):**
        - Replaced SLIP, and provides error correction, compression, and authentication methods
        - Allows TCP/IP to transmit over voice lines
        - Encapsulates messages and transports over serial line
        - Provides communication links between routers, users, and internet PoPs
        - PPP is encapsulated with IP then tunneled to travel over the Internet
- **Tunneling Protocols:**
    - **Point-to-Point Tunneling Protocol (PPTP):**

        - Microsoft protocol allowing remote users to establish PPP then a VPN
        - Encryption is typically employed, but not by default
        - Uses Microsoft Point to Point Encryption (MPPE): MS-CHAP, EAP, or TLS
        - Generic Routing Encapsulation (GRE) | Only works on IP networks
        - Replaced SLIP, which did not provide any of the CIA triad
    - **L2TP:**
        - Same as PPTP, but can tunnel through non-IP networks
        - Doesn't include authentication or encryption
        - Supports TACACS+ and RADIUS (PPTP doesn't)
- **Authentication Protocols: (**Authenticate an identity claim over the network)
    - **Password Authentication Protocol (PAP):**
        - Least secure authentication protocol
        - Authentication by ID and password in CLEARTEXT
        - Prone to a replay attack, replaying username & passwords
        - Authentication server maintains a database of authorized users
    - **Challenge Handshake Authentication Protocol (CHAP):**
        - Reasonably secure authentication protocol
        - Relies on a shared secret, the password, which is stored on the CHAP server
        - User sends UserID in to server in a login request
        - Server verifies user is known, and sends challenge (random value) to user
        - User encrypts random value with their password as the key
        - Server decrypts and compares. If values match access is granted
    - **Extensible Authentication Protocol (EAP):**
        - Most secure authentication protocol. Is part of 802.1X (NAC) | Layer 2 authentication
        - EAP Client, supplicant, requests authentication to a server, called an authenticator
        - Framework that allows other authentication methods to be used (Multi-factor, Kerberos)
            - **LEAP:** Cisco-proprietary, pre-dates 802.1X. Lots of security flaws
            - **EAP-TLS:** Uses PKI. Secure TLS tunnel. Most Secure. Complex & costly
            - **EAP-TTLS**: Simplifies EAP-TLS by dropping client-side cert requirement
            - **PEAP:** Similar to EAP-TTLA (no client-side cert needed) | Uses passwords

Wireless Communications: Use CSMA/CA (collision avoidance) | Transmit information via radio waves or light

- **Spread Spectrum Technologies:** Signal spread across allowable frequencies (faster)
    - **Frequency Hopping Spread Spectrum (FHSS):**
        - Bandwidth split into sub-channels. Hops from one channel to another at interval
        - Difficult to eavesdrop
    - **Direct Sequence Spread Spectrum (DSSS):**
        - Uses sub-bits (Chips) to scramble messages, and Receiver reassembles when received
        - Sequence traffic is unintelligible without Chipping sequence
        - Uses all bandwidth available | Uses all channels at once
    - **Orthogonal Frequency-Division Multiplexing (OFDM):**
        - New multiplexing method
        - Allows simultaneous transmission using multiple independent wireless frequencies
- **Wireless Authentication:**
    - **Open System Authentication (OSA):** No keys needed, and no encryption
    - **Shared Key Authentication (SKA):** Handshake method for authentication
        - **WEP:** Weak. Provides little integrity or confidentiality
        - **WPA:** Better security than WEP | Uses RC4 for confidentiality & TPIK for integrity
        - **WPA2 (RSN):** 802.11i implementation | Uses AES for confidentiality & CCMP for I
- **Wireless Standards:**
    - 802.11: 2 Mbps | 2.4GHz | Sometimes called 802.11-1997
    - 802.11b: 11Mbps | 2.4GHz
    - 802.11a: 54Mbps | 5GHz | European | short range (25')
    - 802.11e: QoS
    - 802.11f: Roaming

- 802.11g: 54Mbps | 2.4GHz
- 802.11h: European
- 802.11i: Includes EAP and 802.1x. AES and TKIP | Robust Security Network (RSN)
- 802.1x: Port-based NAC | Ensures user authentication | Dynamic keys and initialization vectors
- 802.11j: Attempt at worldwide standard
- 802.11n: 100Mbps | 5GHz | Multiple Input, Multiple Output (MIMO)
- 802.15: Wireless Personal Area Network (WPAN) | Bluetooth | 1-3Mbps | 10 Meter range
- 802.16: Metropolitan Area Wireless (broadband wireless)

Secure Remote Access:

- **ISDN:** Early attempt at providing digital service over analog "last mile" phone lines
- **DSL:** Like ISDN, but higher speeds
-

Type	Download Speed	Upload Speed	Distance from CO
ADSL	1.5–9 mbps	16–640 Kbps	18,000 feet
SDSL	1.544 mbps	1.544 mbps	10,000 feet
HDSL	1.544 mbps	1.544 mbps	10,000 feet
VDSL	20–50+ mbps	Up to 20 mbps	<5,000 feet

Laws & Ethics:

Terms & Definitions:
Ethics: Doing what is morally right
Due Care: Requires organizational stakeholders carry out duties according to "Prudent man rule"
Due Dilligence: The management of Due Care. Establishing controls to meet due care
Entrapment: Law Enforcement persuading someone to commit a crime they would not have normally committed
Enticement: Law Enforcement persuading someone to commit a crime they were already intent on committing
Exigent Circumstances: Justification for seizure of evidence without a warrant, b/c it would have been destroyed
Hearsay: Second hand evidence, as opposed to direct evidence. Computer based evidence is typically hearsay
Attribution: Tying a crime to the perpetrator in a court of law

Major Legal Systems:

- **Civil Law:**
  - Most common legal system
  - Leverages codified laws or statutes to determine what is within the bounds of the law
  - Legislative branch creates laws
  - Judicial branch interprets existing laws
  - Judicial precedents DON'T carry weight
- **Common Law:**
  - **Most Testable**
  - Used in the US, Canada, UK, and most former British colonies
  - Legislative branch creates new laws
  - Judicial branch interprets existing laws, and can supersede laws created by Legislative branch
  - Laws change with society, because of judge's influence on them
  - Judicial precedents carry significant weight
- **Religious Law:**
  - Religious doctrine or interpretation is source of legal statutes and understanding
  - The degree to which religious texts & practices are consulted varies greatly
  - Islam is the most common source for religious legal systems (Sharia)
- **Customary Law:**
  - Customs/Practices so commonly accepted by a group they are treated like law
  - Can be later codified as law, but must first be accepted by the group
  - The concept of "Best Practices" is associated with Customary Law

Common Law Branches:

- **Criminal Law:**
  - **Victim**: society itself
  - **Goal**: Deter crime, punish offenders, and maintain an orderly citizenry
  - **Prosecutor:** Government
  - **Burden of Proof:** High. Crime must be proved beyond reasonable doubt
  - **Penalties:** Financial, Incarceration, or Death
- **Civil Law (Tort Law):**
  - **Victim**: Individual, group, or organization
  - **Goal**: To compensate victims who have been harmed by someone else not exercising due care
  - **Prosecutor**: Private Party
  - **Burden of Proof**: Low. A preponderance of proof (It's more likely than not they're guilty)
  - **Penalties**: Financial
    - **Statutory:** Damages prescribed by law, regardless of actual loss or injury
    - **Compensatory:** Financial award to compensate for loss or injury from wrongdoing
    - **Punitive:** Punishing an individual or organization. Used to discourage similar behavior
- **Administrative Law (Regulatory Law):**
  - Law enacted by government agencies (The Executive Branch)
    - Not required to seek input from the Legislative Branch, but must operate within the law

        - Administrative laws can still be scrutinized by the Judicial Branch
    - Used for government-mandated regulations such as FCC, FDA, FAA, and HIPAA Regulations

Computer Crime:

- **Types of Computer Crimes:**
    - **Computers as Targets:** Computer systems are the primary target (ex. DDoS attack)
    - **Computers as Tools:** Computer is central component enable the commission of a crime (ex. Compromising a database to steal customer credit card data) Card data is the target, not the DB.
    - **Computer used Incidentally:** Computer was used, but irrelevant (Killer blogging about murder)
- **Prosecution Difficulties:**
    - **Attribution:** Tying a crime to a perpetrator. Meeting the burden of proof when prosecuting criminal computer crimes is very difficult due to spoofing, malware, botnets, etc.
    - **Jurisdiction:** Attacks bounce off systems in several countries, all with different crime laws and rules of jurisdiction. Some countries won't cooperate
        - **Council of Europe Convention on Cybercrime:** Treaty signed & ratified by the US and 47 European countries, for international cooperation in computer crime prosecution

Intellectual Property: Intangible property resulting from a creative act

- **Types of Intellectual Property**
    - **Trademark:** For Marketing (name, logo, symbol, image). ®: Registered | TM: Unregistered
    - **Servicemark:** A type of Trademark used to brand a service offering
    - **Patent:** Provide a monopoly on an invention (use, make, sell) for 20 years, then becomes public
    - **Copyright:** Protects form of expression of ideas (not the ideas themselves) in artistic, musical, or literary works. © Good for the life of the author +70 years (95 corp). Software licensing is protected by copyright
        - **First Sale:** Copyright limitation allowing the original purchaser to later sell it to another person
        - **Fair Use:** Copyright limitation allowing some limited duplication of the work without payment
    - **Trade Secrets:** Any business-proprietary information providing a competitive advantage (ex. special sauce), which is protected by the business using due care and due diligence. NDA & Non-Compete agreements are common protections
    - **Software Licenses:** A contract between software provider and consumer (ex. EULA)
- **Attacks on Intellectual Property:**
    - Software Piracy
    - Copyright infringement of music & movies
    - Corporate espionage to gain trade secrets
    - Counterfeiting
    - Trademark Dilution: Unintentional. Where a trademarked brand is used generally (ex. Kleenex)
    - CyberSquatting: Someone else registering or using, in bad faith, a trademarked domain name
    - TypoSquatting: Where CyberSquatter registers common typos & misspellings of domain names

Import/Export Restrictions:

- **(CoCom) Coordinating Committee for Multilateral Export Controls:** A multinational agreement not to export certain technologies, including encryption, to communist countries during the cold war
- **Wassenaar Agreement:** The Post-Cold War multinational agreement restricting export for certain technologies, including encryption, to non-member countries. Less restrictive than the former CoCom

Privacy:

- **Key Privacy Question: Are Privacy Protections Opt-In or Opt-Out?**
    - **Opt-In:** No action required by the individual to have their information remain private
    - **Opt-Out**: Individual must do something in order to prevent their information from being shared
- **European Union Data Protection Directive:** The EU's privacy stance
    - Notify individuals of how their personal data is collected & used
    - Allow individuals to opt-out of sharing their personal data with 3rd parties

  - Requires individuals opt-in to have their most sensitive personal data shared
  - Provides reasonable protections for personal data
- **(OECD) Organization for Economic Cooperation & Development:**
  - 30-member nations (including US)
  - A forum in which member countries focus on issues impacting the global economy
  - Issues consensus recommendations that cause changes to policy & legislation worldwide
  - **Protection of Privacy and Transborder Flows of Personal Data:**
    - OECD guideline providing a framework for the protections that should be used when personal data traverses world economies
- **8 Driving Principles Regarding the Privacy of Personal Data:**
  - **Collection Limitation Principle:** Obtain lawfully, and tell individual when possible
  - **Data Quality Principle:** Personal data should be complete, accurate & maintained
  - **Purpose Specification Principle:** Purpose of collection is known & collector is bound to it
  - **Use Limitation Principle:** Don't disclose personal data without consent or legal requirement
  - **Security Safeguards Principle:** Personal data should be reasonably protected from disclosure
  - **Openness Principle:** Policy concerning collection & use of personal data should be available
  - **Individual Participation Principle:** Individuals can find out if/what information is held
  - **Accountability Principle:** The entity using the personal data must adhere to the above
- **EU-US Safe Harbor:**
  - A framework allowing privacy data form the EU to be shared with US companies, even though the US has less stringent privacy laws than the EU
  - US companies must voluntarily comply with the EU Data Protection Directive Principles in order to participate and receive personal data
- **US Privacy Act of 1974:**
  - Codified the protection of US citizens' data that is being used by the US federal government.
  - Defined guidelines regarding how PII would be Collected, Used, and Distributed

Liability:

- Determining whether an organization is legally liable for specific actions or inactions
- Due Care and Due Diligence are the common standards used in determining corporate liability
  - **Due Care:** Uses the "Prudent Man" Rule. Defines a minimum standard of protection that business stakeholders must attempt to achieve
  - **Due Diligence:** The management of Due Care. Following a formal process to ensure their practices meet or exceed the minimum requirements for protection
  - **Negligence:** If a company is found not to have met the minimum standards of Due Care, they are considered Negligent

Legal Aspects of an Investigation:

- **Digital Forensics:**
  - A formal approach to investigations and evidence, aimed at meeting legal requirements
  - Evidence-centric, and closely associated with crimes
  - Preserves the 'crime scene' and evidence, so not to violate the integrity of the data
  - Antiforensics make forensics more difficult (ex malware that is solely memory resident)
  - **LiveForensics:** Acquiring volatile data for forensic analysis
  - **Forensic Process Phases:**
    - Identify potential evidence
    - Acquire that evidence: Create a binary backup
    - Analyze that evidence: Analyze the forensically sound binary backup
    - Produce a report of findings
  - **Binary Copies:**
    - Forensic teams typically take a binary (bit-by-bit) copy of the drive & work off the copy
    - Binary copies copy the entire drive, not just active partitions and used space
    - **Binary copy tools:** EnCase, dd, Windd, and FTK
    - **Drive Space:**
      - **Allocated Space:** Portions of disk marked as actively containing data

        - **Unallocated Space:** Not active, but may contain data from deleted files
        - **Slack Space:** The unused portion of a cluster (minimum size chunk allocated)
        - **Bad blocks/clusers/sectors:** Attackers can mark areas bad to hide data there
- **Incident Response:**
    - Dedicated to identifying, containing, and recovering from security incidents
    - Every response action taken and output received must be documented, in case it goes to court
- **Evidence:**
    - Evidence should be relevant, authentic, accurate, complete, and convincing
    - **Types of Evidence:**
        - **Real Evidence:** Tangible, physical objects (ex. knife)
        - **Direct Evidence:** Testimony by a witness of what they directly experienced
        - **Circumstantial Evidence:** Provide details regarding circumstances that allow assumptions to be made regarding other types of evidence. Indirect proof
        - **Corroborative Evidence:** Provides additional support for a fact called into question
        - **Hearsay:** Second-hand evidence. Normally Inadmissible in court.
            - Business and computer generated records are generally considered hearsay
            - They are admissible only when kept in the course of regularly conducted activity
            - Forensic reports & Binary disk and physical memory images are also admissible
    - **Best Evidence Rule:** Prefers originals over copies, Real evidence over oral testimony, etc.
    - **Secondary Evidence Rule:** Common in computer cases. Copies of originals, computer-generated logs and documents, etc.
    - **Evidence Integrity:** Maintain integrity of data during acquisition & analysis (hashing/checksums)
    - **Chain of Custody:** Requires that once evidence is acquired, full documentation regarding who, what, when, and where evidence was handled is maintained. Supports evidence integrity
    - **Reasonable Searches:** Generally require probably cause and a search warrant
        - **Exigent Circumstances:** When there is an immediate threat of evidence being destroyed, or of a threat to human life, search/seizure can occur without a warrant
        - **Color of Law Enforcement:** Private citizens carrying out actions or investigations on behalf of law enforcement (agents). Search warrants apply here
        - **Search Warrants Not Required:** When law enforcement is not involved, but people should be made aware in advance that they are subject to search
- **Entrapment:** Law Enforcement persuading someone to commit a crime they wouldn't have committed
- **Enticement:** Law Enforcement persuading someone to commit a crime they were intent on committing

Important Laws & Regulations:

- **(HIPAA) Health Insurance Portability and Accountability Act:**
    - Protects Protected Health Information (PHI) from unauthorized use or disclosure
- **Computer Fraud and Abuse Act:**
    - One of the first US computer crime laws
    - Criminalized attacks on protected computers
    - Most major cybercriminals who were convicted were prosecuted under this act
- **Identity Theft Enforcement and Restitution Act:**
    - Removed the $5,000 damage requirement under the Computer Fraud and Abuse Act
    - Made damaging 10 or more computers a felony
- **(ECPA) Electronic Communications Privacy Act:**
    - Protected electronic communications from warrantless wiretapping
- **PATRIOT Act of 2001:**
    - Expanded law enforcement's electronic monitoring capabilities. Weakened ECPA restrictions
    - Less oversight on law enforcement for data collection
- **(GLBA) Gramm-Leach-Bliley Act:**
    - Requires financial institutions to protect the confidentiality & integrity of customer financial info
- **California Senate Bill 1386:**
    - One of the first State-level breach notification laws
- **(SOX) Sarbanes-Oxley Act of 2002:**
    - Created regulatory compliance mandates for publicly traded companies (financial disclosure)

- **(PCI-DSS) Payment Card Industry Data Security Standard:**
  - Payment card vendors attempt to protect cardholder data through self-regulating card processors
- **US Breach Notification Laws:** Currently only state-level laws exist
  - Currently, only state-level laws exist
  - Requires notifying affected parties when their personal data has been compromised
  - States vary regarding what is breach-reportable data

Ethics:

- **Computer Ethics Institute:**
  - **Ten Commandments**
  - Thou shalt not use a computer to harm other people
  - Thou shalt not interfere with other people's computer work
  - Thou shalt not snoop around in other people's computer files
  - Thou shalt not use a computer to steal
  - Thou shalt not copy or use proprietary software for which you have not paid
  - Thou shalt not use other people's computer resources without authorization or compensation
  - Thou shalt not appropriate other people's intellectual output
  - Thou shalt think about social consequences of the program or system you're designing
  - Thou shalt always use a computer in ways that ensure consideration and respect for humans
- **(IAB) Internet Activities Board Code of Ethics and the Internet:**
  - **Five Principles**
  - Don't seek to gain unauthorized access to the resources of the Internet
  - Don't disrupt the intended use of the Internet
  - Don't waste resources (people, capacity, computer) through such actions
  - Don't destroy the integrity of computer-based information
  - Don't compromise the privacy of users
- **ISC2 Code of Ethics:**
  - **Preamble:** Safety of the commonwealth, duty to our principals (employers, contractors, people we work for), and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.
  - **Canons:**
    - **Protect society, the commonwealth, and the infrastructure**
      - Promote and preserve public trust and confidence in information and systems
      - Protect society, the commonwealth, and the infrastructure
      - Promote and preserve public trust and confidence in information and systems
      - Promote the understanding and acceptance of prudent information security measures
      - Preserve and strengthen the integrity of the public infrastructure
      - Discourage unsafe practice
    - **Act honorably, honestly, justly, responsibly, and legally**
      - Tell the truth; make all stakeholders aware of your actions on a timely basis
      - Observe all contracts and agreements, express or implied
      - Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order
      - Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence
      - When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service
    - **Provide diligent and competent service to principals**
      - Preserve the value of their systems, applications, and information
      - Respect their trust and the privileges that they grant you
      - Avoid conflicts of interest or the appearance thereof
      - Render only those services for which you are fully competent and qualified
    - **Advance and protect the profession**
      - Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons

- Take care not to injure the reputation of other professionals
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others