* **Domain 1 Security and Risk Management 16% (1st)**
  + KGI (Key goal indicators)
    - Define measurable goals that tell management after the fact if things were achieved.
  + KPI (Key Performance Indicators)
    - Define measures that determine how well the IT process is performing in enabling the goal to be reached.
  + KRI (Key Risk Indicators)
    - Metrics that demonstrate the risk that an organization is facing or how risky something is.
    - Gives early warnings to identify potential events that may harm the continuity of a project, process or organization.
  + Risk Management
    - Risk Mitigation
      * Removing the risk EX: Patching, encryption etc
    - Risk Transference
      * Insurance or Cloud party
    - Risk Acceptance
      * Just accepting the risk and doing nothing about it
    - Risk Avoidance
      * Not accepting a system or process that may cause a risk to be introduced.
    - Risk Management Maturity model.
      * Sponsor and management.
      * Identify risk.
      * Analyze risk.
      * Plan risk response.
      * Integrate risk management and project management systems.
      * Trust in and a culture of risk management
  + RACI Chart
    - Responsible
      * The person or team responsible for completing a task.
    - Accountable
      * The person ultimately accountable for the correct and thorough completion of the task.
    - Consulted
      * The people who provide input before the work is done.
    - Informed
      * The people who are kept informed on the progress of the task.
  + Governance, risk management, compliance (GRC)
    - Governance – ensures IT goals and processes aligns with business objectives.
    - Risk management – the process of identifying, assessing, and responding to risk.
    - Compliance – conforming to a stated requirement.
      * Laws regulations, auditing, ethics, and privacy
    - All these ties into each other.
  + NIST SP 800-53 REV 5
    - Security and privacy controls for information systems and organizations
    - Primarily for US federal systems very useful even if not in a federal system
    - Select and implement controls and perform risk assessments.
    - It is organizational wide and aligns with many other NIST publications.
    - Control families – focus on a specific aspect of security and privacy.
    - Control classes – management, operational, technical.
    - Baseline controls – the minimum level of security in a system.
    - Outcome based approach.
    - More focus on supply chain management
    - Protection against insider threats
    - The inclusion of privacy controls.
  + NIST SP 800-37 REV 1 and 2
  + Types of attackers/attacks
    - Hackers
      * White – professional pen testers
      * Black – malicious hackers
      * Gray/Grey – in the middle of black and white
      * Script Kiddies – little to no knowledge but uses hacking tools that are easy to use and download.
    - Outsiders – unauthorized individuals (48 – 62%) of attacks.
    - Insiders – (38-52%) most often the weakest link
    - Hacktivist – political or socially motivated purpose
    - Government – state sponsored hacking is common often between the hours of 9-5
    - Bots and Botnets – computer that has been infected with malware when it comes to botnets usually a C&C (Command and Control) controlled by people.
    - Social Engineering
      * Phishing – Wide net to everyone in an organization
      * Spear Phishing – To a specific person/department
      * Whaling – usually to director level or hire individuals.
      * Vishing – voice phishing/phone call
  + Business continuity planning
    - The process of creating the long-term strategic business plan, policies and procedures for continued operations after a disaster
    - COOP (continuity of Operations Plan), crisis communications plan, critical infrastructure protection plan.
    - NIST 800-34 has BCP steps
    - The steps of developing a BCP is:
      * Project initiation
      * Scope the project
      * Business impact analysis
      * Identify preventive controls
      * Recovery strategy
      * Plan design and development
      * Implementation, training, testing
      * BCP/DRP Maintenance
  + BIA Business Impact Analysis
    - RPO (recovery point objective)
      * The acceptable amount of data that can’t be recovered.
    - MTD (Maximum Tolerable Downtime)
      * System rebuild time. The amount of time the system is not operational.
      * MTD >= RTO + WRT
    - RTO (Recovery Time Objective)
      * The amount of time to restore a system.
    - WRT (Work Recovery Time)
      * How much time is required to configure a recovered system.
    - MTBF (Mean time between failure)
      * How long on average will it take for a system to fail.
    - MTTR (Mean time to repair)
      * How long to recover said system.
    - MOR (Minimum operating requirements)
      * The minimum requirements for critical system to operate.
  + The intent of the UC Electronic Communications Privacy Act of 1986 (ECPA) was to protect electronic communications against warrantless wiretapping.
  + When an attacker uses code injections, they are primarily targeting the integrity aspect of the CIA triad. Code injection attacks such as SQL injections, script injections, or command injection, exploit vulnerabilities in an application to introduce malicious code that can modify the systems data and behavior. This undermines the integrity of the data and application logic by allowing unauthorized modifications.
  + ALE (Annual Loss Expectancy) is a concept in quantitative risk analysis that estimates the monetary loss that can be expected for an asset due to a risk over a one-year period. ALE is calculated by multiplying the SLE which is the cost of a single risk event and ARO which is the expected frequency of that event occurring in a year.
  + when it comes to protecting intellectual property in order for it to be protected you need to get a patent or trademark it.
  + ISO 27799 is focused on protecting PHI.
  + When you are looking at the Risk, Vulnerabilities, and threats you are using qualitative risk analysis.
  + A risk analysis matrix is a tool used in qualitative risk analysis that helps in assessing the probability of risk occurring and their impact on the organization.
  + When complying with HIPAA in the United States you must follow the privacy rule and the breach notification rule.
  + COSO (Committee of Sponsoring Organizations) provides a widely accepted framework for internal control and is designed to help organizations evaluate and improve their internal control systems.
* **Domain 2 Asset Security 10% (5th)**
  + The information lifecycle
    - Data Acquisition
      * The information is either created or copies from another location.
    - Data Use
    - Data Archival
      * Retention required by law, or the data will be used later.
    - Data Disposal
      * How do we dispose properly of the data once it is no longer useful
  + Data has 3 states.
    - Data at Rest (Stored Data)
      * Data on disk, tapes, CDs/DVDs, USB Sticks.
      * We use disk encryption which can be hardware or software.
    - Data in Motion (Data being transferred on a network)
      * We encrypt our network traffic, end to end encryption, this is both on internal and external networks.
    - Data in use (We are actively using the files/data, it cannot be encrypted)
      * Use good practices:
        + Clean Desk policy, print policy, no shoulder surfing, locking computer screen.
  + Data Handling (Admin Control)
    - Only trusted individuals should handle data.
  + Data Storage
    - Where do we keep our sensitive data?
  + Data Retention
    - Data should not be kept beyond the period of usefulness or beyond the legal requirements (Whichever is greater)
    - Regulations (HIPAA or PCI-DSS) may require a certain retention of the data (1, 3, 7 years or infinity)
    - Each Industry has it’s own regulations and company policies.
  + Data Custodians
    - These are the technical hands-on emplyees who do the backup, restores, patches, and system configuration. They follow the directions of the data owner
    - A data custodian holds the highest responsibility for data security, ensuring availability, integrity and enforcing security protocols from owners or management.
  + Mission/business owner:
    - Senior executives make the policies that govern data security
  + Data/Information owners:
    - Management level, they assign sensitivity labels and backup frequency
  + System Owner
    - Management level and the owner of the system that houses data
  + Data Controllers and processors
    - Create and manage sensitive data in organization.
  + Security Admins create accounts and assigns access to the data following the data owners directions.
  + Data Remanence – data left over after normal removal and deletion of data
  + Memory – is just )s (off) and 1s (on) switches represent bits
  + ROM (Read only Memory) – is nonvolatile (retains memory after powerloss) (BIOS)
  + PROM (Programmable read only memory)
  + EPROM (Erasable Programmable memory)
  + EEPROM (Electrically erasable programmable read only memory)
  + PLD (Programmable logic devices)
  + the process used to evaluate and approve the security controls of an information system before it is put into operation is known as certification.
  + Flash Drives use EEPROM
  + To protect Data in Use you could implement:
    - Clean Desk Policy
    - Workstation locking
    - Print policy
    - View Angle Privacy screen for monitors
  + When conducting data disposal you are trying to get rid of data remanence
  + If data can cause damage to national security it is considered confidential.
  + During the E-Discovery process, one of the key steps is to produce electronic information or evidence that is relevant to the case to internal or external attorneys or legal teams. This involves identifying, collecting, preserving, reviewing, and sharing electronic data that can be used in legal proceedings.
  + When assigning sensitivity levels to data the data storage format should not be considered.
* **Domain 3 security architecture and engineering 13% (2nd)**
  + Security Models fundamental concepts
    - DAC (Discretionary access control) – gives subjects full control over objects they have created or been given access to
    - MAC (Mandatory Access Control) – System enforced access control based on a subjects clearance and an objects labels
    - RBAC (Role Based Access Control) – is where access to objects is granted based on the role of the subject
    - ABAC (Attribute Based Access Control) – where access to objects is granted based on subjects, objects, and environmental conditions.
      * Attributes could be:
        + Subject (User)
        + Object (Resource)
        + Environment, Locations etc.
        + Threat levels
    - RUBAC (Rule Based Access Control) is granted based on IF/THEN statements.
    - Bell-LaPadula (MAC) – the primary goal of this is to protect data confidentiality
      * Simple security property “No Read Up”
      * Security property “No Write DOWN”
      * Strong \* property “No Read or Write UP and DOWN.”
    - BIBA (MAC)
      * Simple Integrity Axiom “No Read Down”, “No Write up”, “No Read or write up”
      * Focused on integrity not confidentiality.
    - Lattice Based Access Control (LBAC)
      * A Subject can have multiple access rights.
      * A subject with top secret would be able to access everything in the specific layer.
    - Graham – denning model uses objects, subjects, and rules
      * There is 8 rules.
    - HRU (Harrison, Ruzzo, Ullman)
      * An operating system level computer security model that deals with the integrity of access rights in the system.
      * It is an extension of the graham denning model.
      * Uses six primitive operations.
    - Clark Wilson – Integrity:
      * Separates the users from the back end data
      * Separation of duties
      * Well-formed transactions.
      * From one consistent state to another consistent state
    - Brewer Nash model – Chinese wall or information barriers
      * Designed to provide controls that mitigate conflict of interest in commercial organizations and is built upon an information flow model.
    - Non-interference model
      * Ensures that any action that takes place at a higher level does not interfere with actions that take place at a lower level.
    - Take grant protection model.
      * Uses rules that govern the interactions between subjects and objects
      * Contains 4 rules:
        + Take, grant, create, remove.
    - Access control matrix
      * Model describing the rights of every subject for every object in the system.
    - Zachman framework
      * For enterprise architecture
    - Dedicated security mode
      * All users must have
        + Signed NDA, Proper clearance, formal access approval, need to know.
    - System high security mode
      * All users must have
        + Signed NDA, Proper clearance, formal access approval.
    - The orange book is the trusted computer system evaluation criteria
    - The red book is the trusted network interpretation
  + Evaluation methods, certification, and accreditation
    - ITSEC (The European information technology security evaluation criteria)
      * First successful international model
    - The international criteria (ISO/IEC 15408)
      * Common criteria evaluations are performed on computer security products and systems.
      * TOE (Target of Evaluation) the product or system that is the subject of the evaluation
      * PP (protection profile) a document which identifies security requirements for a class of security devices.
      * Security Target (ST) – the documents that identifies the security properties of the target of evaluation. The ST must have one or more of the PPs
    - Evaluation Assurance levels (EAL)
      * EAL Level 1-7
        + 1 functionally tested
        + 2 structurally tested
        + 3 Methodically tested and checked
        + 4 methodically designed, tested, and reviewed.
        + 5 semi-formally designed and tested.
        + 6 semi formally verified design and tested.
        + 7 formally verified design and tested.
  + Secure Design principles
    - Defense in depth, least privilege, need to know etc.
    - Secure defaults – a program or system is as secure as possible when implemented. We can then remove security for usability.
    - Fail Securely – systems are designed to prevent or mitigate unsafe consequences if the system fails.
    - Keep it simple – keeping our security simply makes it better understood and accepted.
      * the more complex security is the harder it is to control, troubleshoot, and manage.
    - Threat modeling
      * PASTA (attacker focused)
        + Process for attack simulation and threat analysis.
        + A seven-step process to aligning business objectives and technical requirements.
        + Gives us dynamic threat identification, enumeration and scoring process.
      * STRIDE (Developer focused)
        + Spoofing, tampering, repudiation, information disclosure, Dos, elevation of privilege.
      * TRIKE (Acceptable risk focused)
      * Dread
        + Disaster/Damage, reproducibility, exploitability, affected users, and discoverability (DREAD)
        + Each category is given a rating from 1 – 10.
    - Secure Design principles
      * Trust but verify
        + Implicit trust but we verify
      * Zero Trust
        + Never trust always verify
        + NIST 800-207
      * Privacy by design
        + Proactive not reactive, privacy by default setting.
      * Shared Responsibilities
        + With cloud computing provider and customer shared responsibilities for security.
    - Secure system design concepts
      * Layering – separates hardware and software functionality into layers.
        + Layers can influence layers next to themselves but not past that.

Nothing to do with OSI model.

* + - * Abstraction – hide unnecessary details from the user it provides a seamless experience for users.
      * Security Domains – a list of objects subjects are allowed to access
        + Kernel mode (supervisor mode)

Allowing low-level unrestricted access to memory, cpu, disk ETC

* + - * + User Mode (problem mode)

No direct access to hardware it is directed through an API

* + - * + Open system – use open standards and can use standard components from multiple vendors
        + Closed systems – use proprietary hardware and software this is security through obscurity.
      * The ring model
        + 4 ring mode separates users (ring 3) form kernel (Ring 0)
        + Slow and rarely used.
  + Northbridge and southbridge
    - More common on new computers.
  + BIOS – basic input output system (low level OS)
    - The Bios runs the basic POST.
      * The kernel loads and execute and the OS boots.
  + WORM Media (Write Once Read Many)
    - ROM is a WORM Media.
  + Trusted Platform Module (TPM)
    - Is an international standard for a secure crypto processor
    - TPM can be used for RNG (Random Number Generation, Symmetric encryption, asymmetric encryption, hashing algorithms, and secure storage of crypto keys and message digest
  + Data Execution Prevention (DEP)
  + Containerization (OS Level Virtualization)
    - Removing redundant OS elements on a VM
  + Elasticity
    - Resources expand or contract based on need.
  + Scalability
    - We scale resources to meet expected needs.
  + The Kernel
    - At the core of the OS is the kernel. At ring 0 or (3) is interfaces between the operating system and applications and the hardware.
  + A monolithic kernel is one static executable, and the kernel runs in supervisor mode.
  + A microkernel are modular kernels. A microkernel is smaller and has less native functionality than a monolithic kernel. You can add functionality via loadable kernel modules.
  + Linux/Unix
    - Read (r), Write (W), and execute (X) permissions which can be set and an owner group or world level.
  + Windows NTSF
    - Windows things
  + The primary advantage of containerization for businesses is that is allows for faster deployment and updates of applications.
  + Virtualization
    - Many Clients on the same hardware
    - Cost less
    - Much easier to setup
    - Easier to snapshot/backup servers
    - Lower power
  + Hypervisor Type 1
    - Bare metal – is part of a virtualization OS that runs on the host hardware
  + Hypervisor type 2
    - Runs on top of host OS
  + VM escape
    - When an attacker can jump from the host tor client to another client.
  + Hypervisor security – if an attacker can get access to the hypervisor they may be able to gain access to the clients
  + Resources Exhaustion – admins oversubscribe the CPU/Memory and do not realize more is needed
  + Cloud Computing
    - When we use cloud computing we build or outsource some part of the IT infrastructure, storage, application.
    - Mostly done because of cost
  + Private cloud
    - Organizations build and run their own cloud infrastructure
  + Public cloud computing
    - Massive infrastructure and everyone can rent it out as they need or want it.
  + Hybrid cloud computing
    - A mix of private and public cloud computing an organization can choose to use private cloud for sensitive information and public for non-sensitive data
  + Community cloud computing
    - Only for use by specific community of consumers
  + IAAS (infrastructure as a service)
    - The vendor provides infrastructure up to the operating system, the customer adds the OS and up.
    - This includes Data Center, Networking, Storage, servers, and virtualization.
  + PAAS (Platform as a service)
    - The vendor provides pre-configured operating systems then the customer adds all the programs and applications.
    - This goes from data center all the way to security.
  + SAAS (Software as a service)
    - The vendor provides the OS and application/programs. Either the customer interacts with the software manually by entering data on the SaaS page or data is automatically pushed from your other applications to the SaaS applications. (Gmail, office 365, Dropbox etc.)
  + Grid computing – can make use of resources not currently in use from 100 or 100,000 computers to perform very complex tasks.
  + Peer to Peer network – any system can be a client or server.
  + Emanations – any unintentional information bearing signals which is intercepted and analyzed could lead to compromise.
  + Covert channels – creates the capability to transfer information using channels not intended to do so.
  + Steganography – hiding a message in another media.
  + Digital watermarks – encode data into a file. Often used to fingerprint files.
  + The most likely vulnerability of an ICS would be unpatched software. Due to ICS operating on older platforms with very specific configurations and software dependencies, regular patching, and updates difficult.
* **Domain 4 communication and network security 13% (4th)**
  + Simplex is a one-way communication one system transmits the other listens.
  + Half Duplex – one can send the other can send both cannot go at the same time (think walkie talky)
  + Full Duplex – both sides can send and receive at the same time.
  + The internet is just a bunch of ISPs connected.
  + Intranet is private organizations with a network.
  + Circuit switching – expensive, but always available, used left often. The circuit guarantees full bandwidth.
  + Packet switching – cheap but no capacity guarantee very widely used today.
  + QoS (quality of service) gives specific traffic priority over other traffic.
  + Most commonly.
  + Personal Area Network – personal network at home probably like a printer, Bluetooth, usb devices etc
  + Local Area Network – a network that connects computers and devices in a small geographic area like the house, office, school etc
    - Everything on it is called a node
  + Metropolitan Area Network – A network covering an entire city, military base, college campus etc
  + Wide Area network – a computer that covers a city, country or spans even intercontinental.
  + VPN – a vpn network sends private data over an insecure network, most often the internet.
  + Global Area Network – A global area network is a network used for supporting mobile users across several wireless LAN’s, satellite coverage areas.
  + The OSI Model
    - There are 7 layers in this model
      * 1 physical – bits
        + Cables, Tangible Topologies, Radio Waves
        + Threats include Data emanation, theft, sniffing, interference.
        + If they say secure, then it is fiber.
        + If they say cheap it is copper
        + If they say cheap and secure, then it is fiber.
      * 2 data link – frames
        + Logical link control
        + Threats

MAC Spoofing, MAC Flooding,

* + - * + ARP (address resolution protocol)
        + CSMA/CD – ethernet – minimized with switches vs hubs
        + CSMA/CA – wireless
        + Token Passing – similar to the talking stick

Not really used anymore

* + - * 3 Network – packets
        + This is where your IP addresses are.
        + Protocols

IP, ICMP, IGMP, IKE, ISAKMP, IPX

If the exam ask which layer 3 protocol starts with I the answer is any of them besides IMAP.

* + - * 4 Transport – segments
        + SSL/TLS Layer 4 to 7
        + UDP – connectionless

Anything real time. Timing is more important than delivery confirmation.

Attacks

Fraggle Attack (DDoS with spoofed packets)

* + - * + TCP – Connection oriented

Will ensure you get all the message reassembled at the destination.

Attacks

Syn Floods

Client server authentication = Syn, Syn/ack, Ack

This is reliable and guaranteed delivery like online banking or anything that needs a guarantee.

TCP uses flags (9 bits – 1 bit flags)

* + - * 5 session – data
        + Establoshes connection between 2 applications
      * 6 presentation – data
        + Only layer with no protocols
      * 7 application – data
        + Presents data to suer (Application/Websites)
        + HTTP, HTTPS, FTP, SNMP, IMAP, POP and Many more
    - This model is used less now and is more a reference point.
  + TCP/IP Model
    - The link Layer – communication methods (Layer 1 and 2 OSI)
    - The internet Layer – connecting independent layers (Layer 3 OSI)
    - The transport Layer – (Layer 4 OSI)
    - The application layer (Layer 5, 6, 7 OSI)
  + SSL is most often used at layer 6 of the OSI model because the presentation layer handles the delivery and formatting of information for the application lahyer processing.
  + Frames and bits are the PDU’s of the Link and Physical layer of the TCP/IP model.
  + MAC Address (BIA)
    - A unique identifier on the network card
    - Can be spoofed pretty easily both for good and less good reasons
    - EUI/MAC-48 are 48 bits
      * The first 24 is manufacture identity
      * The last 24 are unique to the hose
    - EUI-64 Mac Addresses use 24-bit for manufacture but 40 for unique ID
    - Both are widely used today and used by both IPv4 and IPv6
  + Ports
    - 0 -1023 – mostly used for protocol
    - 1024 – 49151 – vendor specific applications
    - 49152 – 65535 – can be used by anyone for anything
  + MPLS (multiprotocol label switching)
    - Directs data from one node to the next based on shot path labels and not IP addresses
    - MPLS can create end to end circuits across any medium
  + SD-WAN
    - Software defined wide area network
    - Higher and cheaper bandwidth, flexibility and scalability of bandwidth allocation
    - Almost instant failover between connection types
    - Easier centralized management
    - Uses IPsec and next gen firewalls.
  + DNP3 (Distributed network protocol)
    - A set of communication protocols used between components
    - It plays a crucial role in SCADA environments
  + SAN (Storage area network)
    - Cost effective way to use the current network infrastructure for storage.
  + FCoE (Fiber Channel over ethernet)
    - The fiber channels HBA are unique cards to interface with storage. Can be combines with the NIC
  + FCIP (Fiber Channel over IP)
    - Encapsulates fiber channel frames via TCP/IP
  + VSAN (Virtual Storage Area Network)
    - A collection of ports from a set of connected fiber channel switches.,
  + iSCI (internet small computer system interface)
    - Leverages existing network infrastructure and protocol to interface with storage.
    - Uses the higher layers of the TCP/IP model
    - Can be used for storage across a WAN
  + VoIP
    - UDP traffic
    - Delivers voice communications over IP networks
  + 802.11 standard
    - A 1997
    - B 1999
    - G 2003
    - N 2009
    - AC 2013
    - AX 2021
* **Domain 5 Identity and Access Management 13% (7th)**
  + Access control is determined by policies, procedures and government standards.
    - This outlines how we grant access to who to what.
      * We use least privilege, need to know and we give our staff and system exactly the access they need and no more.
  + NEVER USE A SINGLE ACCOUNT FOR MULTIPLE USERS.
  + Identification
    - Your name, username, ID Number, employee number, SSN etc!
  + Authentication
    - Should always be MFA.
      * Something you know (Type 1) passphrase, pin, etc
      * Something you have (Type 2) ID, Passport, smart card, token etc
      * Something you are (Type 3) Biometrics, Fingerprint, Iris scan, facial geometry etc
  + FRR (False Rejection Rate) Type 1 error
  + FAR (False accept rate) Type 2 error.
  + CER (Crossover Error Rate) where FRR and FAR meet.
  + Authentication Protocols
    - Kerberos – works with tickets, named after 3 headed dog that guards haiti
      * Builds on symmtrick keys and relies on a trusted third party
      * Used UDP port 88
      * Easy to use and administor
      * Cons if someone compromises it then they have access to everything.
* **Domain 6 Security Assessment and Testing 12% (3rd)**
  + Static testing – we passively test the code, but we do not run it
  + Dynamic testing – we test code while executing it.
  + Fuzzing – a black box testing that submits random, malformed data as inputs into software programs to determine if they will crash.
  + Pen testing – paying someone to test our security by trying to compromise out safeguards.
  + Synthetic Transactions/Monitoring – Building scripts or tools that simulate normal user activity in an application.
  + Security Assessments
    - A full picture approach to assessing how effective our access controls are, they have a very broad scope.
    - Policies, procedures and other admin controls
    - Assessing real world effectiveness of admin controls
    - Change management
    - Architecture review
    - Pentesting
    - Vuln assessment
    - Security Audits
  + Security Audits
    - A test against a published standard
    - Internal, External, and 3rd party audits:
      * (internal) Unstructured Audits – Internal Auditors to improve security and find flaws.
      * External Audits – like internal audits. An external company audits the controls to find flaws and improve security posture.
      * Structured Audit (3rd Party) – External Auditors who validate compliance, often done by a regulatory body, they are experts, and the audit adds credibility.
    - SOC1 – focues on service organization controls relevant to internal control over finance reporting.
      * Type 1 – Opinion on design effectiveness of controls. Type 1 covers single point in time.
      * Type 2 – opinion on design and reporting effectiveness of controls. Type 2 covers a minimum of a six month period.
    - SOC2 – Assess internal controls for compliance and operations. Must meet trust service criteria defines by AICPA: Security, Availability, Process Integrity, Confidentiality, and Privacy. SOC2 Reports are available to management and others under strict NDA it is not widely public.
      * TYPE 1 – report on managements descriptions of a service organizations system and the suitability of the design of controls. Type 1 covers a single point in time.
      * TYPE 2 – report on managements description of a service organizations system and the suitability of the design and operating effectiveness. Minimum of 6-month time period.
    - SOC3 – Similar to SOC 2 but much more generalized, shorter, and a less sensitive document. More public facing document includes only auditors’ opinion and description of controls.
    - Risk = threat \* Vulnerability
    - Pen testing steps:
      * Discovery
      * Gaining Access
      * Escalate privilege.
      * System Browsing
      * Install Additional Tools
    - Test Strategies
      * Planning – Reconnaissance – Scanning (Enumeration) – Vulnerability Assessment – Exploitation – Reporting
  + Pentesting tools
    - Kali Linux
    - Metasploit
    - ****
    - Above is a nice list of Links that have tools you can use?
  + Software Testing
    - Security should be part of software design not an afterthought.
    - Static Testing
      * Looking at the raw code (it is not running)
    - Dynamic Testing
      * Running the program and seeing what happens
    - White box software testing
      * The tester has access to all source code
    - Black Box Software testing
      * Only have the software and no details
    - Regression testing
      * Finding defects after a major code change has occurred.
    - Installation testing
      * Assures that the system is installed correctly and working at the customers hardware.
    - Fuzz testing
      * Testing that provides a low of different inputs in order to try and cause unauthorized access or cause the application to enter an unpredictable state or crash
    - All-pairs testing (Pairwise testing)
      * Defines by black box test design in which test cases are designed to execute all possible DISCRETE combinations of each pair of input parameters.
    - Misuse testing
      * Executing Malicious act against a system. Attackers won’t do what normal users would.
    - Test coverage analysis
      * Done after all testing is complete.
      * Spot check important areas and ensures no major areas are missed.
    - Integration testing is where we progressively test larger and larger groups of software components.
    - After system browsing during a pen test you move onto discovery and installing additional tools
    - During the enumeration phase of a pen test you are scanning systems
    - A vuln scan helps up find outdated software, missing patches and system misconfigurations.
    - In software testing component interface testing would test data handling passed between different unit or subsystems.
    - When a pentester has full admin rights to the system it is called white box testing, but it can also be called clear box or crystal box.
    - A Soc 2 audit reports on the sustainability of the design controls of a network
    - At the end of a software development project when doing interface testing you are testing all interfaces exposed by the application.
* **Domain 7 Security operations 13% (8th)**
  + Key terms for Domain 7
    - Business Continuity Plan
      * Long-term plan to ensure the continuity of business operations in a disaster event.
    - Disaster Recovery
      * Policies, procedures and tools to recover from a natural, environmental or man made disaster.
    - Collusion
      * an agreement between two or more individuals to subvert the security of a system
    - COOP (Continuity of Operations Plan)
      * A plan to maintain operations during a disaster
    - Disaster
      * Any disruptive event that interrupts normal system operations.
    - DRP (Disaster Recovery Plan)
      * Short Term plan to recover from a disruptive even, this is part of the BCP
    - MTBF (Mean Time Between Failure)
      * How long a new or repaired system or component will function on average before failing.
    - RAIN (Redundant Array of Independent/Inexpensive Disks)
      * Using multiple disk drives to achieve greater data, reliability, speed and fault tolerance
    - Mirroring
      * Complete duplication of data to another disk, used by some levels of RAID
    - Striping
      * Spreading data writes across multiple disks to achieve performance gains, used by some levels of RAID.
  + Administrative Personnel Controls
    - **These all help protect against insider threats** 
      * Least Privilege
        + We give employees the minimum aces they need, no more or no less.
      * Need to know.
        + Even if you have access if you do not need to know then you should not access the data.
      * Separation of duties
        + More than one individual in one single task is an internal control intended to prevent fraud and error. We do not allow the same person to enter the purchase order and issue the check.
      * Job Rotation
        + To detect errors and fruads. It is easier to detect fraud and there is less change of collusion between individuals
      * Mandatory Vacation
        + Done to ensure one person is not always performing the same task, someone else has to cover and it can keep fraud from happening or help us detect it.
    - NDA (Non-disclosure Agreement)
      * Employment agreement will include a clause restricting employees use and dissemination of company-owned confidential information.
    - Background Checks
      * References, Degrees, Employment, Criminal History (less Common, more costly)
      * For sensitive position (Classified) the background check is an ongoing (continuous) process.
    - Privilege monitoring
      * The more access and privilege an employee have the more we keep an eye on their activity. With more access comes more responsibility and the higher ability to become a threat.
    - Privileged Account/Access Management (PAM)
      * Account (account safeguarded) Vs. Access (Account + What can the account access/do)
      * We want to identify and monitor anyone with more access than the normal user. The higher privileges they have the closer they should be monitored.
      * We monitor what/when/how/why/where of what is accessed.
      * Full monitoring, limit privileges, MFA, Monitor remote connections, logs/records are immutable, anomaly detection, continuous monitoring, full visibility of all admins and no group accounts.
    - Logging – Managing all logs from our applications and infrastructure the raw data.
    - Monitoring – Making sure that our applications and infrastructure is available and responds to user request within an acceptable time frame, alerts us of issues, the data being used
    - Threat Intelligence
      * Threat Feeds – a stream of raw current and potential threats. We can use the feed to get actual usable data such as domains, malware hashes, malicious code and flagged IP’s.
      * Threat Hunting – actively looking for threats on the network. We assume attackers can access our network and have not been detected. We aggressively search systems for any threat indicator.
    - User and entity Behavior analytics (UEBA)
      * Machine learning to model typical and atypical user behavior setting a baseline to identify an attack or malicious user.
  + **Administrative Security** 
    - Digital Forensics
      * Focuses on the recovery and investigation of material found in digital device, often in relation to computing crime.
        + Forensics Process

Identify the potential evidence, Acquire the evidence, analyze the evidence, make a report.

* + - * The evidence must be accurate, complete, authentic, convincing, admissible.
      * Identify – what is left behind.
      * Preservation – Chain of custody, write blockers, make a hash.
      * Collection – examine and analyze the data, document everything and handle the evidence as little as possible.
        + Work from most volatile to least.
      * Real Evidence – tangible and physical objects, in IT Security – Hard drives, USB Drives – not the data on the device
      * Evidence integrity – it is vital the evidence integrity cannot be questioned
      * Chain of custody – this proves the integrity of the data, no tampering was done.
      * Artifacts – evidence/digital traces left behind from an attacker
      * Continuous monitoring – just what it sounds like
      * NIST 800-53 RMF
        + Six Steps

Step 1 – Categorize

Step 2 – Select

Step 3 – Implement

Step 4 – Assess

Step 5 – Authorize

Step 6 – Monitor

* + - Spinning Disk Forensics
      * Allocates space
        + The portions of the disk that are marked as actively containing data
      * Unallocated Space
        + The portions of the disk that does not contain active data. This is parts that havenever been allocated and previously allocated parts that have been marked as unallocated.

If space was previously allocated and you deleted the data it is not actually gone until it is overwritten

* + - * Slack space
        + Data is stored in specific sized chunks known as clusters (Clusters = sectors or blocks). A cluster is the minimum size that can be allocated by a file system. If a file does not use the whole cluster then the left over space in the cluster is slack space.
      * Bad Blocks/Clusters/Sectors
        + Hard disk end up with sectors that cannot be read due to some physical defect. The sectors marked as bad will be ignored by the operating system since no data could be read in those defective portions

Attackers can mark sectors or clusters as being bad in order to hide data within this portion of the disk

* + - Network Forensics
      * A sub branch of digital forensics where we look at the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Network investigations deal with volatile and dynamic information.
      * Usually has two issues:
        + The first type is monitoring a network for anomalous traffic and identifying intrusions (IDS/IPS). An attacker may be able to erase log files on compromised host, a network-based evidence might be the only evidence available for forensic analysis.
        + The second type relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords, and parsing human communication such as emails or chat sessions.
      * Catch as you can.
        + All packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage.
      * Stop, look, and listen.
        + Each packet is analyzed in a basic way in memory and only certain information is saved for future analysis. This approach requires a faster processor to keep up with incoming traffic.
      * Embedded device forensics
        + We have decades of analyzing and investigating standard systems, traffic, and hardware but embedded devices is a new player. They include SSD’s, GPS, Cellphones, PDA and much more. They contain a lot of information.
      * Forensic software analysis
        + Comparing or reverse engineering software. Reverse engineering malware is one of the most common examples. Investigators often try to have a binary copy of a malware program and try to deduce what is actually does.
      * Egress Monitoring
        + Done to prevent data exfiltration both logically and physically. For logical egresss monitoring we can use DLP systems. For physical egress we could use guards and make sure the trash cannot be removed from the organization without being monitored.
      * Electronic discovery (E-Discovery)
        + The discovery in legal proceedings, litigation, government investigations, or freedom of information act request, where the information is in electronic format.
    - **Incident Management** 
      * Involves the monitoring and detection of security events on our systems, and how we react in those events. This is an administrative function of managing and protecting computer assets
      * Incidents and events can be categorized into 3 classes:
        + Natural – flood, hurricanes, earthquakes, blizzards, anything that is caused by mother nature
        + Human – Done intentionally or unintentionally by humans these are the most common.
        + Environmental – this is not nature, but the environments we work in, the power grid, the internet connections, hardware failures, software flaws etc
      * Event
        + An observable change in state, this is neither negative nor positive, just something has changed.
      * Alert
        + Triggers warnings if certain event happens
      * Incident
        + Multiple Adverse events happening on our systems or network, often caused by people.
      * Problem
        + Incidence with an unknown cause, we would follow similar steps to incidence response. More time would be spent on root cause analysis.
      * Inconvenience (Non-disaster)
        + Non-disruptive failures, hard disk failure, 1 server in a cluster is down.
      * Emergency (Crisis)
        + Urgent, event with the potential for loss of life or property
      * Disaster
        + Our entire facility is unusable for 24 hrs or longer.
      * Catastrophe
        + Our facility is destroyed.
      * Incident management 8 step lifecycle
        + Preparation

This is where we write policies, train staff, get proper hardware etc

* + - * + Detection (Identification)

Events are analyzed to determine if they might be a security incident. If we do not have strong detection methods then we may not realize we have a problem until it is to late,

* + - * + Response (Containment)

The response phase is when the response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of an incident. This can be taking a system off the network and etc

Make bit level copy of things.

* + - * + Mitigation (Eradication)

This is where we remove attack vectors, backdoors, malware etc

* + - * + Reporting

We report throughout the process beginning with detection and start reporting immediately.

* + - * + Recovery

Restore the system back to operational status and continue to monitor the system.

* + - * + Remediation

The remediation happens during the mitigation phase where vulnerabilities on the impacted system are mitigated.

* + - * + Lessons learned (post-incident activity, port mortem, or reporting)

Assume problem is fixed and everything is back online. So, this phase is where we can learn from mistakes, compromises, what went well or what did not.

Root cause analysis is supposed to be done here as well.

* + - **Preventive and detective controls**
      * We use IDS and IPS on the network to capture and alert or block traffic seen as malicious.
      * They can be categorized into 2 types and 2 different approaches towards identifying malicious traffic:
        + Network based. – placed on a network segment (a switch port in promiscuous mode).
        + Host based – on a client usually a server or workstation.
        + Signature (Pattern) Matching – like AV it matches traffic against a long list of known malicious traffic patterns.

Much faster and super easy to setup and configure. But these are vulnerable to zero day attacks because they only know current or known attacks

* + - * + Heuristic-Based (Behavioral) – uses normal traffic patterns baseline to monitor for abnormal traffic. The larger picture, for full picture views and data correlation we use a SIEM or a SOAR.

Takes a while to build baselines.

* + - * + Hybrid based – looks for signatures and behavioral base.
      * IDS
        + They are passive, they monitor but they take no further actions.
      * IPS
        + They act after detection.
      * IDS/IPS
        + Part of layered defense just packet sniffers
      * Network based – placed on a network segment so all traffic is caught. Can protect against DDos and port scans.
      * Host based – single system monitoring. We can see unencrypted traffic.
      * Fragmentation – sending fragmented packets so the signature is not detected.
      * Avoiding default – switching ports or finding ways around countermeasures.
      * Address spoofing/proxying – attackers use poorly secured proxy service.
      * Pattern change evasion
  + **SIEM and SOAR systems** 
    - SIEM
      * Provides holistic view of our organization’s events and incidents. Gathers from all systems and looks at everything.
    - SOAR
      * A software solution that uses AI to allow us to respond to some security incidents automatically.
  + **Application positive listing**
    - Positive listing (whitelisting)
      * Basically, allowing the application we want to run in our environment.
    - Removable media controls
      * Locking down USB ports, CD Drives, memory card ports and anything else where you could load malicious data onto the system from external devices.
  + **Honey pots and Honeynets**
    - Honey pots
      * System looking like a real system but with the sole purpose of attracting attackers. Used both internally and externally.
      * Need approval from senior management and legal department.
        + Remember entrapment and enticement.
    - Honeynets is just a group of honey pots.
  + **Configuration Management** 
    - To make systems more secure we would have a baseline to harden the servers.
      * This should not be manual because it creates the ability to miss which is why we should have an image.
    - Before putting a system in production, we should do a vulnerability scan and patch scan.
  + **Patch management** 
    - In order to keep the network, secure we need to apply patches on a regular basis.
    - 2nd Tuesday of the month (Patch Tuesday)
    - Patch management is a corrective control.
    - You want this to be automated as much as possible. But you also want to ensure you do this properly.
  + **Change management** 
    - Formalized process on how to handle changes in an environment.
    - If done right we will have full documentation, testing and everything done before presenting it to the board.
    - Process for change management is as follows:
      * Identify change.
      * Propose the change.
      * Assess the change.
      * Provisional change approval
      * Testing the change
      * Scheduling the change
      * Change notification
      * Implementation
      * Post implementation
    - Change management process
      * Plan
        + Request, analyze, approve (CAB)
      * Do
        + Plan implementation, communicate, implement and test.
      * Check
        + Success, failure (rollback
        + Communicate
      * Act
        + Acceptance, lessons learned.
  + **Zero-day vulnerability** 
    - Vulnerabilities not generally known or discovered; the first time an attack is seen is considered 0 day. Hence the name.
    - 0-day vulnerability – the vulnerability that has not been widely discovered and published
    - 0-day exploit – code that uses the 0-day vulnerability
    - 0-day attack – the actual attack using the code.
    - Stuxnet work used 4 unique zero-day exploits.
      * A worm
        + Spreads
      * A link
        + Auto execute.
      * A rootkit
        + Hide itself and processes.
  + **Backups** 
    - Fault tolerance – to ensure internal SLA’s and provide as high availability as possible we use a high degree of redundancy and resiliency as makes sense to that particular system and data set.
    - Full backup – everything
    - Incremental – back up what was changed since last backup
    - Differential – backup everything that has been changed since the last full backup
    - Copy backup – full backup but includes the memory and the flash
  + **BCP and DRP** 
    - BCP
      * This is the process of creating the long-term strategic business plans, policies, and procedures for continues operation after an event.
      * This is for entire organization not just IT.
      * COOP falls under BCP.
      * Crisis communications, DRP, ISCP, all fall under BCP
    - DRP (disaster recovery plan)
      * This is the process of creating the short-term plans, policies, procedures and tools to enable the recovery or continuation of vital IT systems in a disaster.
      * DRP is a subset of BCP.
    - **Cyber Security is everything online IT security is everything.**
    - Natural
      * Anything caused by nature.
    - Human
      * Anything caused by humans.
    - Environmental
      * Anything in our environment, power outage etc.
    - Electrical or power problems (environmental)
    - Heat (Environmental)
      * 68 – 77 Fahrenheit is the recommended temp
    - Pressure (environmental)
    - Humidity (Environmental)
    - **DRP Lifecycle** 
      * Mitigation
      * Preparation
      * Response
      * Recovery
    - Remember to assign calls to positions/roles and not people.
    - Rescue team (activation/notification)
      * Responsible for dealing with disaster as it happens.
        + Evacuate employees etc
    - Recovery Team
      * Responsible for getting the alternate site up and running as fast as possible.
    - Salvage Team (Failback)
      * Responsible for getting systems and staff back to primary site.
    - BIA (Business Impact Analysis)
      * Identify critical and non-critical systems, functions and activities!
      * RPO
        + The acceptable amount of data that can not be recovered.
      * MTD (maximum tolerable downtown)
        + The time to rebuild the system and configure it for reinsertion into production must be less than or equal to the MTD
      * RTO (Recovery time objective)
        + The amount of time to restore the system hardware.
      * WRT (work recovery time)
        + How much time to recover software on system.
      * MTBF (mean time between failure)
        + How long a new or repaired system or component will function on average before failing.
      * MTTR (Mean time to repair)
        + How ong it will take to recover a failed system
      * MOR (Minimum operation requirements)
        + The minimum environmental and connectivity requirements
    - COOP (Continuity of operations)
      * How we keep operating in a disaster. How do we get staff to new location, etc
    - Cyber incident response plan
      * How we respond to cyber events usually in the DRP
        + This could be DDos, worms.
    - OEP (Occupant Emergency plan)
      * How do we protect our facilities, our staff and the environment in the event of a disaster.
    - Walk/Talk-through (Tabletop or structured walkthrough)
      * A group of managers and critical personal sit down and talk through the recovery process
    - Read through
      * Managers and functional areas go through the plan and a check a list of components needed for the recovery process.
    - Simulated test (Walkthrough drill)
      * Similar to walkthrough but the team simulates the disaster and the team respons with thir pieces from the DRP
    - Physical Tests:
      * Parallel Processing
        + We bring critical components up at a secondary site using backups, while the same systems are up at the primary site, after the last daiy backup.
      * Partial interruption
        + We interrupt a single application and fail it over to secondary facilities
      * Full interruption
        + We interrupt all application and fail it over to our secondary facilities.
* **Domain 8 Software Development Security 10% (6th)**
  + Waterfall Software Development Methodologies
    - Very Linear, each phase leads directly into the next
      * System Requirements, Software Requirements, Preliminary Design, Detailed Design, Code and Debugging, testing, operations and maintenance.
    - The unmodified waterfall model does not allow us to go back to the previous phase.
  + Sashimi Model
    - Waterfall with overlapping phase. If we close one phase, we add the next phase. This is a modified waterfall that lets us go back.
  + Agile Software Development
    - Describes a set of values and principles for software development under which requirement and solutions evolve through the collaborative effort of self-organizing cross functional teams.
    - Based on the agile manifesto which has twelve principles.
  + Scrum
    - Is a framework for managing software development. Scrum is designed for teams of roughly 10 people. Daily standup meetings
    - The product owner
      * Represents the product stakeholders which wis the voice of the customer.
    - Dev team
      * Responsible for delivering the product.
    - The scrum master.
      * Facilitates and accountable for removing roadblock and teams are responsible for what they are doing there job.
  + XP (Extreme Programming)
    - Intended to improve software quality and responsiveness to change and this uses 2 people writing the code.
  + The Spiral model
    - A risk driven process model for software projects. This has 4 phases planning, risk analysis, engineering and evaluation, plan the next iteration.
  + RAD (Rapid Application development)
    - Puts emphasis on adaptability and the necessity of adjusting requirements in response to knowledge gained as the projects progresses.
  + Prototyping
    - Breaks projects into smaller task. Then we take those and design multiple prototypes, so we have options and the customer and us has a better understanding.
  + The SDLC (Software Development Lifecycle)
    - The SDLC is not really a methodology but a description of the phases in the life cycle of software development.
    - Assume is has security built into process if on the exam it does not mention security it is not SDLC.
  + Projects
    - A temporary endeavor with a finite start and end time. That is focused on creating a unique product, service or result.
  + Program
    - Is a collection of related projects. Like a project a program is temporary when the collection of projects is complete the program is complete.
  + Portfolio
    - Is a collection of projects and programs that are managed as a group to achieve a strategic objective.
  + IPT (Integrated Product Team)
    - A multidisciplinary group of people who are collectively responsible for delivering a defined product or process.
    - Big picture people you want their input, and you want to go back and get input. So, you will need good people skills.
  + Source code escrow
    - The deposit of the source code of software a third-party escrow.
    - This is so that way under certain terms if we need the source code we get the source code. Like if the company goes out of business
  + Source Code repositories
    - Using a public third-party code repositories come with security concerns.
    - Often used by open-source projects and other multi-developer projects to handle various versions.
  + API (application programming interface)
    - Allows an application to communicate with another application, operating systems, databases, networks etc
    - They are a good example of how we integrate for better usability, but often security is overlooked.
  + Software change and configuration management
    - Both change and configuration management are very applicable In software development processes
    - NIST 800-128 guide for security focused configuration management of information systems.
  + DevOps
    - Cooperation between Development, operations and quality assurance.
    - CI/CD (Continuous Integration/Continuous delivery)
      * The D in CD can also refer to as deployment or development.
    - If you are using DevOps in our software development, then you would deply new code daily. Daily deployments are due to continuous integration and continuous deployment practices.
  + DevSecOps
    - Evolved from DevOps to add security into the process. We want security to be implemented into the process.
  + Scaled Agile Frameworks
    - SAFe for Enterprise Agility
      * Aliging Agile teams
    - Efficiency and effectiveness
      * Meeting goals with minimum waster
    - Agile Methodologies
      * Adapting with SCRUM and KanBan
    - Scaling agility
      * Teams, programs, portfolios
    - Agile release trains
      * Coordination and delivery
    - Key components
      * Program increment planning and lean portfolio management
  + Buffer Overflow (Buffer Overrun)
    - An anomaly where a program while writing data to a buffer overruns the buffers boundary and overwrites adjacent memory locations. Happens from improper coding when a programmer fails to perform bound checking.
  + Race Condition
    - When two or more programs may collide in their attempts to modify or access a file
  + TOCTOU (Time of Check to Time of Use)
    - A softwire bug caused by changes in a system between the checking of a condition and the use of the results of that check
  + Privilege escalation
    - Exploiting a bug to gain higher access to a system then you are granted.
  + Ethical disclosure
    - What you do when you discover a vulnerability.
      * Partial disclosure is telling the vendor you found a vulnerability.
  + SOAR
    - Security Orchestration, Automation, and response
    - Uses AI to respond to security incidents.
  + Operation and Maintenance
    - Once software project is handed to operations there will be maintenance task that are required to be completed.
  + In the software capability maturity model some processes are possible repeatable at level 2 with consistent results
  + One of the most effective ways for De-Identifying personal data is by applying statistical techniques to remove identifying characters. Some techniques can include noise addition, permutation, data swapping, and more complex methods like differential privacy.
  + the most important step to take when conducting a regulatory investigation is to document the entire process.
  + CSS is a style sheet language that is used to describe the presentation of a document written in a markup language like HTML.
  + A stateful firewall examines a packet to see if it is the result of a previous connection.
  + Using MAC (Mandatory Access Control) A file, Printer, and Computer would exist as objects. Object when referring to MAC are resources that can be Accessed.
  + Users or groups would exist as subjects because subjects are entities that access objects
  + Digital Timestamps are helpful at preventing replay attacks.
  + A replay attack is when the attacker monitors the traffic stream in a network and maliciously repeats or delays the transmission of valid data over the network.
  + When a TCB failure occurs as a result of a lower privileged process trying to access restricted memory segments the system goes into maintenance mode.
    - Also referred to as an emergency system restart.
  + Corroborative evidence enables you to prove either a point or an idea. Is it additional evidence that is credible and admissible in the court of law.
  + The executive succession plan ensures that vital corporate positions are filled in the event it is vacated during a disaster.
  + Fingerprint systems enroll the entire fingerprint of a user for future authentication attempts.
  + Finger scan systems extract only specific characteristics of the fingerprint and enable faster processing of a user authentication request.
  + Deluge water sprinklers when activated discharge large amounts of water in a short time. These should not be used in a data center.
  + Security analyst is a strategic role that helps to develop policies, standards, and guidelines to ensure the security elements are implemented correctly.
  + A system security policy specifies the list of approved hardware and software. Is also specifies the steps undertaken for the protection of infrastructure equipment.
  + A key schedule is an algorithm that calculates the subkeys for each round of ciphering.
  + An object-oriented database is used to store multiple types of data. Such as images, audio, video, and documents. The data elements and the different components are referred to as objects.
  + The computer security act of 1987 pertains to confidential and sensitive information maintained by federal agencies. This act does not deal with data held by private organizations. The computer security act of 1987 has the following requirements:
    - The federal agency should identify the computer systems that contain sensitive information.
    - A security plan should be developed and implemented for the system’s security.
    - Periodic security awareness training should be conducted for employees.
    - Acceptable computer usage practices should be defined in advance.
    - The government agencies should ensure that employees maintain a certain level of awareness and protection.
  + A privacy notice should be provided via a posted copy, a printed copy at the first service delivery, and a printed copy available upon request by a covered entity to the patient.
  + A business continuity plan is not an operational control.
  + Operational controls ensure the confidentiality, integrity, and availability of business operations by implementing security as a continuous process.
  + The 1991 US Federal sentencing guidelines apply to the following white collar crimes that take place within an organization
    - Antitrust
    - Federal Securities
    - Mail and wire fraud
    - Bribery
    - Contracts
    - Money Laundering
  + The principles underline in the 1991 US federal sentencing guidelines provide a cause of action to the law enforcement agencies dealing with white collar corporate criminals.
  + RADIUS uses port 1812 to communicate with dial up users. It is a UDP based protocol.
  + Disk Mirroring, disk striping with parity, and Failure resistant disk system (FRDS) protects against data loss if a single drive fails. Disk mirroring provides a duplicate cope of the data on the mirrored hard drive. Disk striping with parity rebuilds the lost data using the parity information in the event of a single drive in the array fails. FRDS is sued primarily in file server and is similar to RAID.
  + After identifying resources and information you should also examine the hardware on which the resources and information reside. Operations security examine the countermeasures used to protect resources, information and the hardware on which the resources and information reside.
  + Personal are not option that are examines during operations security. As stated before operations security is to protect information, resources and the hardware for which it resides and neither of these have to do with personal.
  + Orange book level B is considered mandatory and is based on the Bell-Lapadula security model
  + Data Normalization ensures that attributes in a database table depend on the primary key.
  + Normalization is required to prevent repetitive information from appearing in a database.
  + L0phyCrack, John The Ripper, and Crack are all tools used to obtain user passwords.
  + Synchronous Data Link Control (SDLC) and High-Level Data link Control (HDLC) are primarily used to enable IBM mainframes to communicate with remote computers. A synchronous protocol, SDLC, is used over networks with permanent connections. Mainframe environments are generally considered more secure than LAN environments because there are fewer entry points to the mainframe.
  + A proxy server acts as an internet gateway, firewall and internet caching server for a private network. Hosts on the private network contact the proxy server with an internet web site request.
  + You should complete a site survey to ensure that no unauthorized wireless access points are established. Site survey produce information on the types of systems in use, the protocols in use, and other critical information.
  + The primary function of the (COCOMO) the construction cost model is for cost estimation.
  + The primary goal of operations security is to guard against information asset threats generated within an organization.
  + Direct evidence will negate the need for presumption in the court of law. Direct evidence does not require backup information to prove the fact. Therefore, presumption are not required. The testimony of a witness is an example of direct of evidence because the oral testimony of a witness does not require any corroborative evidence to prove the fact.
  + The main purpose of keeping tract of the number and location of backup versions is to ensure proper disposal information.
  + Cross certification is primarily used to establish trust between different PKI’s and build an overall PKI hierarchy. Cross certification allows users to validate each others certificate when they are certified under different certification hierarchies.
  + Stateful firewalls and Packet filtering firewalls operate at the network layer of the OSI model.
  + Authentication is the OSI function that ensures that the identity of the remote host is verified and that the data received is authentic. This process takes place at the session layer of the OSI model.
  + Reduced Instruction set computing (RISC) is computing instructions that are simpler and require less cycles to execute.
  + The three categories of computer crime are:
    - Computer assisted crime – this category is one in which a computer is sues as a tool to carry out a crime.
    - Computer targeted crime – this category is one in which a computer is the victim of the crime.
    - Computer incidental crime – this category of crime is one in which a computer is involved incidentally in the crime. The computer is not the target of the crime and is not the main tool uses to carry out the crime.
  + TCP and UDP both operate at the transport layer of the OSI model, because the transport layer is the fourth layer in the OSI model it is sometimes referre to as layer 4
    - So if asking what is a layer 4 protocol then they are referencing TCP/UDP
  + An implicit deny can ensure that certain users do not have access to a subnet through a router. Users who do NOT have an implicit deny can be allowed to access the subnet.
  + Electronic vaulting backs up data in real time but transmits the data to an offsite facility in batches.
  + RSA is an example of asymmetric cryptography. RSA can prevent MiTM Attacks, RSA Does not deal with Discrete logarithms, RSA is used worldwide de facto standard for digital signatures. RSA uses public and private keys for integrity verification.
  + The Capstone chip implements the US Escrowed encryption standard and was developed by the NSA. It implements the same algorithm as the clipper chip.
  + Trust is a primary concern in directory service domains, Kerberos environments, and distributed environments.
  + The transport layer of the TCP/IP model corresponds to the transport layer of the OSI model.
  + SHA was designed to be used with DSS with this algorithm a message of less than 264 bits is input to SHA. The resultant message digest of 160 bits is fed into the DSA which generates the digital signature of the message.
  + To determine the Single Loss Expectancy of an asset you need to multiple the asset value by the exposure factor
  + If you send a packet with the header of xxx.xxx.255.255 it is going to send a message to all stations on the xxx.xxx network.
  + The protection profile contains a set of security requirements including functionality and assurance criteria for a product and the rationale behind such requirements. The EAL rating intended for the product is also specified. The environmental conditions, the expected functional, the assurance levels and the product objective are also included in the protection profile when the product is evaluated by the Common Criteria for a target evaluation rating.
  + Object linking and embedding database (OLE DB) is the database interface language that is a replacement for ODBC and can only be used by Microsoft windows clients.
  + Administrative law defines regulatory standard for the performance and the conduct of companies. Administrative law is often called regulatory law. This type of law includes considered standards of performance or conduct exected by government agaencies from companies, industries, and certain officials
  + Genetic algorithms are used in evolutionary computing. Evolutionary computing is a type of AI.
  + The audit privilege use audit category will audit all instances of users exercising their rights.
  + A double-blind test is more likely to demonstrate the success or failure of a possible attack. In a double blind test the security team of the network being tested does not know about the test. This test evaluates how the team reacts to the attack.
  + The focus of PaaS cloud deployment is data protection.
  + The main purpose of IKE is to manage the security associations across the network.
  + TGT and AS are responsible for granting tickets in Kerberos.
  + A resident virus is specifically designed to infect programs as they are loaded into the memory.
  + All the users in the dedicates security mode have the clearance and the formal approval required to access all the data process by the system.
  + During the reconstitution phase of a recovery an organization moves back to its original site or to a new site that was constructed to replace the original site.
  + Identification is the method used by a user or process to claim who they are or to assert who they claim to be.
  + If a biometric device is granting access to unauthorized users, then it has a high type 2 error rate and allows the authentication of unauthorized users. (False Acceptance)
  + The mean time between failure (MTBF) is the estimated amount of time that a piece of equipment should remain operational before failure. The MTBF is usually supplied by the hardware vendor or a third party.
  + The noninterference model provides multilevel security and ensures that the commands and activities performed at one security level do not affect the activities at another security level.
  + The multilevel security mode, which is sometimes called controlled security mode, assigns the use of sensitivity labels to subjects and objects to regulate the information flow.
  + Means is used to indicate how a criminal committed the crime.
  + The purpose of quantitative risk analysis is to analyze the already prioritized risk in such a way to give each a numerical rating. Quantitative risk analysis attempts to quantify the prioritization, probability, and effect for security risk. It most often follows qualitative risk analysis.
  + Critical areas should use continuous lighting and be illuminated eight feet in height to two foot candles.
    - According to NIST
  + A capability table is used to display the access rights for a subject pertaining to a certain table. Subjects are bound to capability tables.
  + Shatter resistant glass should be used in the glass panes used for one wall of the data center. This is because the wall will be acting as an exterior wall.
  + Network address translation (NAT) acts as the interface between a local area network and the internet using one public IP address
  + A covert channel is not controlled by a security mechanism. A covert channel is a communication path that accesses information in an unauthorized manner and violates the security policy. A covert channel is not a regulated path of the information flow and is an effect of a software bug or a compromised system.
  + An open system is a system that is built upon standards and protocols from published specifications. Open systems are subject to review and evaluation.
  + A spamming attack involves flooding an email server or specific email addresses repeatedly with identical unwanted emails. Spamming is the process of using an electronic communication medium, such as email, to send unsolicited messages to users in bulk.
  + A system cold start requires intervention of system administrator for system restoration.
  + A 3DES operation can work in the following modes:
    - DES-EEE3 that uses three different keys for encryption.
    - DES-EDE3 that uses their different keys to encrypt, decrypt and then again encrypt the data, respectively. This process makes it the most secure form of 3DES.
    - DES-EEE2 and DES-EDE2 function like DES-EDE3 however they only use two keys. The first and third encryption process uses the same key.
  + A program can operate as both a subject and an object.
  + IP Octet ranges
    - A = 0-126
    - B = 128-191
    - C = 192-223
    - D = 224-239
    - E = 240-255
      * Note the 127 address is uses for loopback.
  + A NAT Router provides a transparent firewall solution between an internal network and outside networks.
  + The security level B2 is referred to as structured protection.
  + Accreditation is not associated with the common criteria.
  + When you are performing the reconstitution phase of recovery you should restore the least critical function to the new primary site first. Then if there are issues with the new site the critical functions of the company are not negatively affected.
  + An open system is a system that is built upon standards and protocols from published specifications open systems are subject to review and evaluation.
  + The term footprint is used to describe the area that is covered by a satellite.
  + The KDC is used to store, distribute, and maintain crypto session keys.
  + Rule based access control uses the setting in pre-configured security policies to make all decisions.
  + WAP Gap occurs in versions of WAP prior to version 2.0 WTLS is replaced by tls in WAP 2.0
  + The WAP GAP issue involved WTLS. It occurs when the gateway decrypts WTLS transmissions and re-encrypts is with TLS/SSL sensitive data can be captured while it is on the gateway.
  + Classification and need to know ensure that information is compartmentalized in the information flow model.
  + Top secret is the highest data classification when it comes to government or military use.
  + A cognitive password is based on some personal fact or opinion.
  + The access provisioning lifecycle includes.
    - Creation
    - Maintenance
    - Deletion
  + The operate and maintain phase of the security management lifecycle includes the following:
    - Ensure that all baselines are met.
    - Complete internal and external audits
    - Complete tasks outlined in the blueprints.
    - Manage service level agreements as outlines in the blueprints.
  + A database management system (DBMS) refers to a suite of software programs that maintains and provides controlled access to data components stored in rows and columns on a table.
  + Certification is a detailed technical evaluation of security components and their compliance prior to formal acceptance.
    - The following processes may be used for certification:
      * Safeguard evaluation
      * Risk analysis
      * Verification
      * Testing
      * Auditing techniques
  + Countermeasures for session management attacks include the following:
    - Implement randomized session ID’s.
    - Implement time stamps or time-based validation.
    - Encrypt cookies that include information about the state of the connection.
  + Software upgrade deployment should not be transferred to the security administrator.
  + The tranquility principle used in the Bell-Lapadula model prevents the security level of subjects and objects from being changed once they have been created. For this reason, the Bell-Lapadula model is very static in nature. The strong tranquility property states that objects never change their security level.
  + A proxy firewall hides a packets true origin before sending it through another network. The primary security feature of a proxy firewall is that it hides the client information. It is the only computer on a network that communicates with untrusted computers.
  + When performing a pentest you should follow the steps as follows:
    - Discovery
    - Enumeration
    - Vulnerability Mapping
    - Exploitation
    - Report
  + As part of the business continuity plan you should consider natural disasters and hardware failure.
  + CHAP uses a challenge response method to authenticate a user. Encrypted authentication applies a digital signature algorithm to the data bits that are sent from the claimant to the verifier. In CHAP, a logon request is sent from the user to the auth server. The server responds by sending a challenge with a random value to the user. The user encrypts this challenge with a predefines password. The server denies or grants access to the user by decrypting the challenge response and comparing it to the value received from the user.
  + Administrative law emphasizes the performance and conduct of organizations.
  + Administrative law defines regulatory standards for the performance and the conduct of companies. Administrative law is often called regulatory law.
  + When there is a fire that has paper, laminates, and wooden structures you use water and soda acid.
  + To prevent against war-driving attacks
    - Change the default SSID.
    - Disable SSID broadcast.
    - Configure the networks to use authenticated access only.
  + Natural Surveillance is the facet of the CPTED approach that is being addressed.
  + When you encrypt confidential data using a computers operating system encryption feature, the data is protected only while it is on the original media. Encryption is enforced on a single drive. Once data is copied to another drive file encryption is no longer used.
  + The advantage of ECC over RSA is its improved efficiency and requirement of fewer resources than RSA. ECC has a higher strength per bit than RSA.
  + IDS systems and audit logs are used to monitor access control violations.
  + The operations team is responsible for preventing problems, reducing hardware and software failures, and reducing the impact of incidents.
  + The disaster recovery plan is primarily concerned with minimizing property damage and preventing loss of life. The most important concern during a disaster is personnel safety.
  + You should implement every computer on the DMZ as a bastion host because any system on the DMZ can be compromised.
  + A bastion host is in essence a system that is hardened to resist attacks.
  + An iris scan can be affected by the sun shining on the reader. The placement of the biometric device used to perform the iris scan is very important.
  + Polymorphism occurs when different objects respond to the same command or input in different ways.
  + A proxy firewall hides a packet’s true origin before sending it through another network.
  + When digital cash is marked as identified the identity of the cash holder is known
  + Memory dumps are admissible in the court of law as evidence to prosecute a suspect. Memory dumps contain the latest state of the system before the attack occurred.
  + The Patriot Act was established in 2001 to reduce restrictions to search telephone, email communications, medical, finance, and other records. Up until the Patriot Act was established law enforcement officials were limited by the fourth amendment.
  + During the preservation phase of the embedded device analysis, you will create hashes, checksums, and document everything.
  + In MAC environment security labels are the most important entity.
  + Ad-hoc reporting is being used when you setup the business intelligence (BI) solution, connect it to data sources, establish security settings, and determine which objects users can access.
  + Using the order of volatility to preserve evidence it should be in this order:
    - Memory (RAM)
    - Network processes
    - System Processes
    - Hard drive
    - Back up tapes
    - DVD’s (Lead Volatile)
  + Circumstantial evidence presents intermediate facts that facilitate the judge and the jury to logically deduce a fact. circumstantial evidence is a fact hat is used to deduce another fact related to the primary matter under consideration.
    - circumstantial evidence requires interference from the available facts.
  + The business continuity plan should be maintained for several reasons including:
    - Infrastructure changes
    - Environmental changes
    - organizational changes
    - hardware, software, and application changes
    - personnel changes.
  + The business continuity plan should not be changes due to budget changes. The plan needs to be left alone no matter the budget.
  + A passphrase is usually the easiest password type to remember.
  + A pass phrase is usually the easiest to remember even though it is longer than a static password it is considered easier to remember because you can make it a sentence.
  + When restoring backups you only need to restore the most recent full back up and then the most recent differential backup.
  + A packet filtering firewall only examines the packet header information.
  + C2MyAzz virus captures user passwords as they are entered into the computer.
  + A redundant site is owned by the company and can be brought online relatively easily. It is also managed by the company usually this site is hot meaning it is ready for production immediately.
  + A hot site is a site owned by another company and can be brought online relatively easily. The company needing the backup services pays a fee to the owner the owner is responsible for management of the hot site.
  + Audit events that should be monitored include logon attempts, account modifications, file modifications. According to the principle of accountability significant events should be traceable to an individual.
    - File creation should not be monitored. Users should be able to create files.
  + RADIUS uses port 1812 to communicate with dial up users.
  + The following statements regarding one-time pads are true
    - Each pad can only be used once
    - The pad must be made up of random values
    - The pad must be as long as the message
    - The pad must be distributed and stored in a secure manner.
  + EAL1 – functionally tested
  + EAL2 – structurally tested
  + EAL3 – methodically tested and checked
  + EAL4 - methodically designed, tested, and reviewed
  + EAL5 – semi-formally designed and tested
  + EAL6 – semi-formally verified design and tested
  + EAL7 – formally verified design and tested
  + Anomaly based is most likely to produce a false alet. With anomaly based monitoring, alets occur where there are any deviations from normal behavior.
  + A rollback operation cancels any database changes from the current transaction and returns the database to it’s previous state. It prevents a transaction from updating the database with partial or corrupt data.
    - Rollbacks occur during the operations/mainentance phase of the SDLC
  + The software protection association (SPA) deals with the prevention of software piracy.
  + The least upper bound and greated lower bound operators control the flow of information in the Lattice based access control model (LBAC)
  + The main focus of a platform as a service (PaaS) cloud computing is data protection.
  + In object-oriented programming (OOP) the method defines the functions that an object can carry out.
  + The testing and development processes should be separated from each other to manage the stability of the test environment. Separating the test environment and the development environment is an example of separation of duties.
    - The person developing should not be testing and the person testing should not be developing.
  + The tranquility principle in the Bell-LaPadula model prevents the security level of subjects and objects from being changed once they have been created. For this reason, the bell-lapadula model is very static in nature. The strong tranquility property states that objects never change their security level.
  + A two-man control implies that two operators review and approve each other’s work. A two-man control reduces the chances of fraud. Therefore, the risk associated with operations involving highly sensitive information is minimized.
  + HIPAA is enforced by the office of civil rights (OCR) of the department of health and human services. (HHS)
  + If you are extracting hidden data from an image, you are in the examination phase of the incident investigation.
  + The examination phase includes traceability, validation techniques, filtering techniques, pattern matching, hidden data discovery, and hidden data extraction.
  + Authorization creep is the term used to describe when a user is assigned additional access permissions because of changing jobs. User permissions should be reviewed on a regular basis to ensure that the enforcement of the least privilege is used.
  + Semantic integrity should be enforced. Semantic integrity ensures that data types and rules are enforced. It includes checking data types, values, data constraints and uniqueness rules. Semantic integrity protects the data by ensuring the data values follow all the rules.
  + EAL 4 is the common benchmark for operating systems and products. Common criteria have designed the evaluation criteria into 7 EAL’s:
    - EAL 1 – a user wants the system to operate but ignores security threats.
    - EAL 2 – developers use good design practices, but security is not a high priority.
    - EAL 3 – developers provide moderate levels of security.
    - EAL 4 – security configuration is based on good commercial development. This level is the common benchmark for commercial systems, including operating systems and products.
    - EAL 5 – security is implemented starting in early design. It provides high levels of security assurance.
    - EA 6 – Specialized security engineering provides high levels of assurance. This level will be highly secured from penetration attackers.
    - Extremely high levels of security are provided. This level requires extensive testing, measurement, and independent testing.
  + The Control objectives for information and related technology (CobiT) is a security framework that acts as a model for IT governance and focuses more on operational goals.
  + The .bat and .cmd extensions are used for naming batch files in a Microsoft environment.
  + As part of the business continuity plan, natural disasters should be considered. Natural disasters include tornadoes, floods, hurricanes, and earthquakes. A business continuity strategy needs to be defines to preserve computing elements, such as the hardware, software and networking elements. The strategy needs to address facility use during a disruptive event and define personnel roles in implementing continuity.
  + Hardware failures should also be considered in a business continuity plan. This hardware can be limited to a single computer component but can include network link of communication line failures. The majority of the unplanned downtime experienced by a company is usually due to hardware failure.
  + Server relocation does not need to be include in the business continuity plan this should be carefully planned out to where it does not affect business operations when it happens.
  + Employee resignation should not be apart of the business plan. Employee resignation is a normal part of doing business. However strikes and the actions of angry employees should be considered.
  + The concealment cipher is based on the clues in the physical factors affecting the sender and receiver. It is based on agreement between the two communicating parties as to which patter to use to determine the actual message.
  + Critical arewas should have continuous lighting and be illuminated eight feet in height and two foot candles.
  + The 100BaseFX ethernet specification uses fiber optic cable, which is immune to crosstalk, EMI, and tapping because it transmits light rather than electricity.
  + In the security management lifecycle if you are identifying assets and change control blueprints you are in the engage phase.
  + PGP establishes a web of trust between users. A web of trust implies that the users generate and distribute their public keys. These keys are signed by users for each other, establishing a community of users who trust each other for communication. Every user has a collection of signed public keys stored in a file known as a key ring. A level of trust and validity are associarted with each key in that list.
  + In a distributed computing environment an agent is a program that performs services in one environment on behalf of a principal In another environment.
  + Ethernet 2 frames include both the MAC Destination and source, they include a two-bye type field and the 802.1Q tag is optional.
  + Disaster simulation testing can be quite involved and should be performed annually. To complete this test you should create a simulation of an actual disaster, including all of the equipment, supplies, and personnel needed. This test will determine if you can carry out critical business function during the event.
  + To determine the SLE Single loss expectancy you should use Asset Value \* Exposure factor.
  + The advantage of ECC or RSA is ECC requires fewer resources.
  + An X.509 CRL contains a list of serial numbers of unexpired or revoked digital certificates that should be considered invalid.
  + You should implement TPM on client computers to best manage encryption keys, passwords, drive encryption, and digital rights for users.
  + NFS, TFTP, and SNMP all use UDP
  + A honey pot should reside on the DMZ or screened subnet.
  + IDaaS should provide:
    - SSO
    - Provisioning
    - Password management
    - Access governance
  + The Business impact analysis is the part of the business continuity plan that involves analysis
  + the flaw hypothesis methodology is used to analyze operating system vulnerabilities in a penetration testing project. The flaw hypothesis methodology refers to a system analysis and penetration testing technique in which specification and documentation for an operating system are analzed to compile a list of possible flaws. The flaw are prioritized according to conditions.
  + ***SECURITY KERNEL!!!!!***
  + Statistical intrusion detector is not a component of an IDS system but a key function performed by an anomaly based IDS.
  + Natural Access Control in the CPTED approach includes door, fence, lighting and landscaping placement. This control ensures traffic is controlled.
  + Start and Stop bits mark the beginning and ending of asynchronous communication.
  + The first step when someone submits a change request is to analyze the change request.
  + A capability table is used to display the access rights for a subject pertaining to a certain table. Subjects are bound to capability tables.
  + Access authorization and auditing are not associated in a properly segregated environment. Approvals for access authorization granted by an individual should be audited by a separate individual. This will ensure the segregation of duties and act as a cross check for monitoring assigned privileges. The auditing component of the IT system should be independent and distinct from the information system security architecture for a system.
  + Cross certification is primarily used to establish trust between different PKI’s and build an overall PKI hierarchy. Cross certification allows users to validate each others certificate when they are certified under different certification hierarchies
  + The primary purpose of cross certification is to build a trust relationship between different certification hierarchies when users belonging to different hierarchies are required to communicate and might require authentication for legitimate connections. The process implies the establishment of a trust relationship between two certificate authorities (CA’s) throught he signing of another CA’s public key in a certificate referred to as a cross certificate.
  + A proxy firewall is considered a second generation firewall.
  + The revocation request grace period refers to the maximum response time taken by the certificate authority (CA) server to perform a revocation. A certificate is revoked either when the information contained in the certificate is supposedly compromised or when a certificate expires. The revocation request can be initiated by the following entities:
    - The certificate holder
    - The CA itself
    - Another CA that issues certificates
    - An associated RA
  + A program can operate as both a subject and an object.
  + Password files are vulnerable to dictionary attacks and brute force attacks.
  + The red book in the rainbow series covers security issues for networks and network components, and databases.
  + Steps in the equipment lifecycle are as follows:
    - Assessment
    - Procurement and deployment
    - Management
    - Retirement
  + SLE is calculated by the asset value multiplied by the exposure factor.
  + MSP is used by the military to secure email messages. It is used to sign and encrypt messages and perform hashing functions.
  + PGP establishes a web of trust between users.
  + Before developing a business continuity plan you should develop the continuity planning policy statement.
  + A multi-level security policy is usually associated with MAC.
  + A Fraggle attacks is when a large amount of UDP packets is sent to a host causing it to crash.
  + Routers operate at the network layer of the OSI model which is layer 3.
  + Identification is used by a user/process to claim who they claim to be.
  + Identification is the method used by a user or process to claim who they are or to assert who they claim to be. Identification involves supplying your username, account number, or some other form of personal identification. It is how a user provides a claim of his or her identity to a system.
  + The tranquility principle used in the Bell-LaPadula model prevents the security level of subjects and objects from being changed once they have been created. For this reason, the model is very static in nature.
  + In a business continuity committee, all business units must be present and senior management must be present as well.
  + TCSEC evaluates the assurance and functionality of a system.
  + When implementing biometrics if you want to use a method that is not super intrusive you can use voice print it is considered to be less intrusive then other methods available.
  + A slot lock uses a slot cable to connect the internal hard drive of a pc to the pc hard drive slot inside the computer.
  + Business continuity is a corrective control. Corrective controls are controls that take corrective action against a threat.
  + Root Cause analysis happens during the review stage of the incident response which is the last stage of the process.
  + Bahvior based monitoring looks for behavior that is not allowed or may be perceived as malicious and acts accordingly.
    - If you define a rule preventing an email client from executing cmd.exe command and to alert you when this is attempted it is considered behavoir based monitoring
  + A double blind test is more likely to demonstrate the success or failure of a possible attack. In this test the security team does not know it is going to happen and the test team does not know how the security team will respond.
  + Backup controls, software testing, and Anti-Virus management are all operational controls.
  + To identify and prosecute cyber criminals and to establish the source of the attack and the chain custody, FBI works in coordination with the secret service and local law enforcement.
  + Software upgrade deployment is something a security admin should not be doing.
  + RADIUS uses port 1812 to communicate with dial up users.
  + The information flow model allows the flow of information between the different security levels and the objects within the same security level based on an access control matric. A flow acts as a type of dependency by relating two version of the same object.
  + The audit privilege use audit category will audit all instances of users exercising their rights. Like logging onto a server or another system using their account.
  + A NAT Router provides a transparent firewall solution between an internal network and outside networks.
  + A port control is a device lock that prevents access to hard drives or unused ports in a computer.
  + A biometric system based on fingerprinting has a low user acceptance level. Users are often reluctant to provide their fingerprint to authenticate.
  + In an information processing facility doors and walls should have the same fire rating.
  + When setting up a virtual environment you should not allow browsing on the internet this can lead to several security issues.
  + Downstream liability ensures that organizations working together under a contract are responsible for their information security management.
  + A proximity detector is a IDS that uses magnetic or electrostatic field to detect intrusions.
  + The following components complement an IDS system:
    - A Vulnerability analysis system (VAS)
    - Honeypots
    - Padded cells
    - File integrity checks
  + An object is an entity in the access control matrix to which subjects can be granted permissions. A column in an access control matrix corresponds to the access control list (ACL) for an object.
  + Cryptanalysis is not used to test the strength of a crypto algorithm.
  + The CSO’s role should be self-governing and independent of all the other departments in the organization.
  + An active hub functions at the physical layer of the OSI model.
    - An active hub or multiport repeater just amplifies or regenerates signals to all other ports on the hub.
  + Macro viruses are programs written in word basic, visual basic, or VBScript. Macro viruses pose a major threat because their underlying language is simple.
  + the steps in designing a business continuity plan are as follows:
    - Identify the plans scope.
    - Identify key business areas.
    - Identify critical functions.
    - Identify dependencies between business areas and critical functions.
    - Determine acceptable downtime.
    - Create the plan to maintain operations.
  + Quantitative risk analysis attempts to predict the likelihood a threat will occur and assigns a monetary value in the event a loss occurs.
  + Open Vulnerability and Assessment language (OVAL) is a standard written in XML that provides open and publicly available security content.
  + Trust is a primary concern with Kerberos, Directory Service Domain, Distributed Environments.
  + The main focus of PaaS cloud computing is data protection.
  + The main focus of SaaS cloud computing is application access management.
  + The main focus of IaaS cloud computing is virtual machine management.
  + A security policy is a preventive admin control.
  + Configuration change should be added to the change log after the change is approved.
  + RADIUS enabled remote access users to log onto a network through a shared authentication database.
  + NIST 800-137 guides the development of information security continuous monitoring (ISCM) for federal information systems and organizations. It defines the following steps to establish, implement and maintain ISCM:
    - Define ISCM strategy.
    - Establish an ISCM program.
    - Implement ISCM program.
    - Analyze data, and report findings.
    - Respond to findings.
    - Review and update the ISCM strategy and program.
  + The presentation layer of the OSI model is responsible for formatting data
  + A NIDS cannot analyze encrypted information
  + If a file server is experiencing unscheduled initial program loads (IPLS) the system is rebooting.
  + A honey pot is a computer used to entice an attacker
  + SKIP is a key distribution protocol.
  + Blowfish is a symmetric algorithm that is considered public domain it can be freely used by anyone.
  + A resident virus is specifically designed to infect programs as they are loaded into the memory.
  + Visibility is one of the considerations involved in identifying a secure location for facility requirement planning. In visibility considerations, you identify the types of neighbors around the chosen location whether the identified location should be marked as a sensitive area to prevent trespassing.
  + A database management system (DBMS) refers to a suite of software programs that maintans and provides controlled access to data components stores in rows and columns on a table.
  + A rollback operation cancels any database changes from the current transaction and returns the database to it’s previous. It prevents a transaction from updating the database with partial or corrupt data. Rollbacks occur during the operations/maintenance phase of the SDLC
  + When travelling with a company owned device you should avoid transporting the devices in checked baggage.
  + When travelling with a company device you should follow these guidelines:
    - Use encryption when possible.
    - Do not leave the device unattended.
    - Do not use public Wi-Fi networks.
  + If you install a network analyzer and it only captures one subnet to capture all the subnets, you could install the network analyzer on all the subnets or install a distributed network analyzer.
  + The Take-Grant Access control model uses states and state transitions in designing and protecting systems. The Take-Grant model was created to show that it is possible to secure a computer even when the number of subjects and objects is large.
  + 802.11b supports a max of 11 mbps
  + Direct evidence will negate the need for presumptions in the court of law
  + Disaster simulation testing can be quite involved and should be performed annually
  + SSL operates at the transport layer of the OSI model
  + Network address translation (NAT) acts as the interface between a local are network and the internet using on public IP address.
  + A capability corresponds o a row in the access control matrix.
  + Stateful firewalls and packet filtering firewalls operate at layer 3 of the OSI model
  + Anomaly based network monitoring is most likely to produce a false positive alert.
  + A backup control is an operational control
  + /etc/hosts.equiv is a file on a unix system that allows user to connect remotely without having to authenticate
  + A time of check/time of use (TOC/TOU) Attack is another name for an asynchronous attack.
  + Rule based access uses the setting in pre-configured security policies to make all decisions.
  + In a Kerberos environment the Key Distribution Cetner (KDC) Is the most important component. It is responsible for managing all the secret keys.
  + NFS, TFTP and SNMP all use UDP.
  + Triple DES (3DES) uses 48 rounds of computation.
  + Disk striping provides only performance enhancements and does not provide fault tolerance. RAID 0 is known as disk striping.
  + L0phtCrack, John the ripper, and crack are all used to obtain user passwords.
  + In Diffie-Hellman key exchange users exchange secret keys over a non-secure medium
  + A packet filtering firewall only examines the packet header information.
  + The density of traffic should be considered during the facility acquisition phase. The facility location must provide easy accessibility to transport services for commuting purposes and to respond to emergency situations.
  + If a hard drive MTTR is to high then you can just add another drive and implement disk mirroring.
  + Chain of custody refers to strict and organized formal procedures in accordance with the law and the legal regulation governing the collection.
  + EAL 4 is the common criteria standards for benchmarks for operating systems and products.
  + Snort is an IDS system.
  + In order to implement RADIUS that allows VOIP you would need to implement it with Diameter.
    - Diameter was created to address new tech that radius was not designed to handle. Including VoIP
  + Drop ceilings pose more of a security threat to a facility infrastructure because if systems and resources are separated then you could use the ceiling to access them.
  + RAID 1 implemented with a single hard disk controller is referred to as disk mirroring. With disk mirroring two hard disk are connected to the same hard disk controller and a complete copy of each file is stored on each disk.
  + RBAC, MAC and CBAC are non-discretionary in nature. Non-discretionary methods are those that rely strictly on security policies or security levels to determine object access.
  + Traverse mode noise is caused by difference between hot and neutral wires
* [**https://www.kaplanlearn.com/offline/qbank/91682091**](https://www.kaplanlearn.com/offline/qbank/91682091) **(DESKTOP)**
* [**https://www.kaplanlearn.com/offline/qbank/91682091**](https://www.kaplanlearn.com/offline/qbank/91682091) **(laptop)**