Domain 1 **Security and Risk Management**

1.1 Understand, adhere to, and promote professional ethics

As a CISSP, you must understand and follow the (ISC)² code of ethics, as well as your organization's own code.

- (ISC)² Code of Professional Ethics. Take the time to read the code of ethics available at www.isc2.org/Ethics (http://www.isc2.org/Ethics). At a minimum, know and understand the ethics canons:
    - Protect society, the common good, necessary public trust and confidence, and the infrastructure. This is "do the right thing." Put the common good ahead of yourself. Ensure that the public can have faith in your infrastructure and security.
    - Act honorably, honestly, justly, responsibly, and legally. Always follow the laws. But what if you find yourself working on a project where conflicting laws from different countries or jurisdictions apply? In such a case, you should prioritize the local jurisdiction from which you are performing the services.
    - Provide diligent and competent service to principles. Avoid passing yourself as an expert or as qualified in areas that you aren't. Maintain and expand your skills to provide competent services.
    - Advance and protect the profession. Don't bring negative publicity to the profession. Provide competent services, get training and act honorably. Think of it like this: If you follow the first three canons in the code of ethics, you automatically comply with this one.
- Organizational code of ethics. You must also support ethics at your organization. This can be interpreted to mean evangelizing ethics throughout the organization, providing documentation and training around ethics, or looking for ways to enhance the existing organizational ethics. Some organizations might have slightly different ethics than others, so be sure to familiarize yourself with your organization's ethics and guidelines.

1.2 Understand and apply security concepts

- **Confidentiality**:
    - Concept of measures used to ensure the protection of the secrecy of data, objects, and resources
    - Confidentiality protections prevent disclosure while protecting authorized access
    - Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and prioprietary information
    - Sensitive data, including personally identifiable information (PII) must be kept confidential. Confidentiality is different from secrecy
    - Preserving confidentiality means protecting an asset or data, even if it's not a secret
- **Integrity**:
    - Concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data
    - Preventing unauthorized subjects from making modifications
    - Preventing authorized subjects from making unauthorized modifications, such as mistakes
    - Maintaining the internal and external consistency of objects

- **Availability**:
    - Authorized subjects are granted timely and uninterrupted access to objects
    - To ensure high availability of services and data, use techniques like failover clustering, site resiliency, automatic failover, load balancing, redundancy of hardware and software components, and fault tolerance
- **Authenticity**: ensuring a transmission, message or sender is legitimate. See the NIST glossary for examples: https://csrc.nist.gov/glossary/term/authenticity (https://csrc.nist.gov/glossary/term/authenticity)
- **Nonrepudiation**:
    - Ensures that the subject of activity or who caused an event cannot deny that the event occurred
    - Nonrepudiation is made possible through identification, authentication, authorization, accountability, and auditing
- **AAA Services**:
    - Identification: claiming to be an identity when attempting to access a secured area or system
    - Authentication: proving that you are that claimed identity
    - Authorization: defining the permissions (i.e. allow/grant and/or deny) of a resource and object access for a specific identity or subject
    - Auditing: recording a log of the events and activities related to the system and subjects
    - Accounting: (aka accountability) is reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions, especially violations of organizational security policy

1.3 Evaluate and apply security governance principles

- **Security governance**: the collection of practices related to supporting, evaluating, defining, and directing the security efforts of an organization.
    - Security governance is the implementation of a security solution and a management method that are tightly interconnected
    - There are numerous security frameworks and governance guidelines, including the National Institute of Standards and Technology (NIST) SP 800-53 and NIST SP 800-100
- **The security function**: the aspect of operating a business that focuses on the task of evaluating and improving security over time. To manage security, an org must implement proper and sufficient security governance
    - the act of performing a risk assessment to drive the security policy is the clearest and most direct example of management of the security function
- **Third-party governance**: external entity oversight that may be mandated by law, regulation, industry standards, contractual obligation, or licensing requirement. Outside investigator or auditors are often involved
- **Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives**
    - **Security Management Planning** ensures proper creation/implementation/enforcment of a security policy, and alignment with organizational strategy,goals, mission, and objectives

    - **Strategic Plan**: a strategic plan is a long-term plan (useful for 5 years). It defines the organization's security purpose. A strategic plan should include risk assessment.
    - **Tactical Plan**: mid-term plan (1 year or less) developed to provide more details on accomplishing the goals set forth in the strategic plan
    - **Operational Plan**: a short-term, highly detailed plan based on strategic or tactical plans
    - Strategy, goals, missions,and objectives — support each other in a heirarchy.
    - **Objectives** are closest to the ground-level and represent small efforts to help you achieve a mission.
    - **Missions** represent a collection of objectives, and one or more missions lead to goals. When you reach your goals, you are achieving the strategy
    - A security framework must closely tie to mission and objectives,enabling the business to complete its objectives and advance the mission while securing the environment based on risk tolerance

- **Organizational Processes**

    - Security governance should address every aspect of an organization, including organizational processes of acquisitions, divestitures, and governance
    - Be aware of the risks in acquisitions (since the state of the IT environment to be integrated is unknown, due diligence is key) and divestitures (how to split the IT infrastructure and what to do with identities and credentials)
    - Understand the value of governance committees (vendor governance, project governance, architecture governance, etc.)
    - Executives,managers and appointed individuals meet to review architecture, projects and incidents (security or otherwise),and provide approvals for new strategies or directions. The goal is a fresh set of eyes, often eyes that are not purely focused on information security
    - When evaluating a third-party for your security integration, consider the following:
        - on-site assessment
        - document exchange and review
        - process/policy review
        - third-party audit

- **Organizational Roles and Responsibilities**

    - Senior Manager: has a responsibility for organizational security and to maximize profits and shareholder value
    - Security Professional: has the functional responsibility for security, including writing the security policy and implementing it
    - Asset Owner: responsible for classifying information for placement or protection within the security solution
    - Custodian: responsible for the task of implementing the proscribed protection defined by the security policy and senior management
    - Auditor: responsible for reviewing and verifying that the security policy is properly implemented

- **Security control frameworks**

    - A control framework is important in planning the structure of an organization's security solution. There are many frameworks to choose from, such as:

        - **Control Objectives for Information Technology (COBIT)** ["moderately referenced" on the exam]
            - COBIT is a documented set of best IT security practices by ISACA
            - Six key principles:
                - Provide stakeholder value
                - Holistic approach
                - Dynamic governance system
                - Governance distinct from management
                - Tailored to enterprise needs
                - End-to-end governance system
        - ISO 27000 series (27000, 27001, 27002, etc.).
        - NIST **CyberSecurity Framework (CSF)**
            - designed for commerical orgs and critical infrastructure, consisting of five functions:
                - identify
                - protect
                - detect
                - respond
                - recovery
    - Due care/due diligence
        - **Due diligence**: establishing a plan, policy, and process to protect the interests of the organization. Due diligence is about understanding your security governance principles (policies and procedures) and the risks to your organization. Due diligence often involves gathering information through discovery, risk assessments and review of existing documentation; developing a formalized security structure containing a security policy, standards, baselines guidlines, and procedures; documentation to establish written policies; and disseminating the information to the organization
        - **Due care**: practicing the individual activities that maintain the due diligence effort. Due care is about your legal responsibility within the law or within organizational policies to implement your organization's controls, follow security policies, do the right thing and make reasonable choices
        - Security documentation is the security policy
        - After establishing a framework for governance, security awareness training should be implemented, including all new hires, who complete the security awareness training as they come on board, and existing employees who should recertify regularly (typically yearly).

1.4 Determine compliance and other requirements

- Understand the difference between criminal, civil, and administrative law.
    - **Criminal law**: protects society against acts that violate the basic principles we believe in. Violations of criminal law are prosectued by federal and state governments
    - **Civil law**: provides the framework for the transaction of business between people and organizations. Violations of civil law are brought to the court and argued by the two affected parties
    - **Administrative law**: used by government agencies to effectively carry out their day-to-day business
- **Compliance**: Organizations may find themselves subject to a wide variety of laws, and regulations imposed by regulatory agencies or contractual obligation

    - **Payment Card Industry Data Security Standard (PCI DSS)** - governs the security of credit card information and is enforced through the terms of a merchant agreement between a business that accepts CC payments, and the bank that processes the business' transactions
    - **Sarbanes-Oxley (SOX)** - financial systems may be audited to ensure security controls are sufficient to ensure compliance with SOX
    - **Gramm-Leach-Bliley Act (GLBA)** - affects banks, insurance companies, and credit providers; included a number of limitations on the types of information that could be exchanged even among subsidiaries of the same corp, and required financial institutions to provide written privacy policies to all their customers
    - **Health Insurance Portability and Accountability Act (HIPAA)** - privacy and security regulations requiring strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store private medical information about individuals; also clearly defines the rights of individuals who are the subject of medical records and requires organizations that maintain such records to disclose these rights in writing
    - **Federal Information Security Management Act (FISMA)** - requires federal agencies to implement an information security program that covers the agency's operations and contractors
    - **Computer Fraud and Abuse Act (CFAA)** (as amended) - protects computers used by the government or in interstate commerce from a variety of abuses
    - **Electronic Communications Privacy Act (ECPA)** - makes it a crime to invade the electronic privacy of an individual
    - **Digital Millennium Copyright Act** - prohibits the circumvention of copyright protection mechanisms placed in digital media and limits the liability of internet service providers for the activities of their users
- **Privacy requirements**
    - European Union's **General Data Protection Regulation (GDPR)** - replaced Data Protection Directive (DPD), purpose is to provide a single, harmonized law that covers data throughout the EU
        - Lawfulness, fairness, and transparency
        - Purpose Limitation
        - Data Minimization
        - Accuracy
        - Storage Limitation
        - Security
        - Accountability
    - California Consumer Privacy Act (CCPA)
    - Be familiar with the EU Data Protection Directive. Be familiar with the requirements around healthcare data, credit card data and other PII data as it relates to various countries and their laws and regulations

1.5 **Understand legal and regulatory issues that pertain to information security in a holistic context**

- **Cybercrime and data breaches**:
    - Understand the notification requirements placed on organizations that experience a data breach
    - California's SB 1386 implemented the first statewide requirement to notify individuals of a breach of their personnel information; all other states eventually followed suit with similar laws
    - Currently, federal law only requires notification of individuals when a HIPAA-covered entity breaches their protected health information (likely to soon change)

    - Before an organization expands to other countries, perform due diligence to understand legal systems and what changes might be required to the way that data is handled and secured
    - In particular, be familiar with:
        - **Council of Europe Convention on Cybercrime** - a treaty signed by many countries that establishes standards for cybercrime policy
        - Laws about data breaches, including notification requirements
        - In the US, the **Health Information Technology for Economic and Clinical Health (HITECH)** Act requires notification of a data breach in some cases, such as when the personal health information was not protected as required by HIPAA
        - GLBA applies to insurance and financial organizations, requiring notification to federal regulators, law enforcement agencies and customers when a data breach occurs
        - Certain states also impose their own requirements concerning data breaches
        - the EU and other countries have their own requirements, for instance, the GDPR has very strict data breach notification requirements: A data breach must be reported to the competent supervisory authority within 72 hours of its discovery
        - Some countries do not have any reporting requirements
- **Licensing and intellectual property (IP) requirements**
    - **Trademarks**: words, slogans, and logos used to identify a company and its products or services
    - **Patents**: a temporary monopoly for producing a specific item such as a toy, which must be novel and unique to qualify for a patent
        - **Utility**: protect the intellectual property rights of inventors
        - **Design**: cover the appearance of an invention and last for 15 years. They don't protect the idea of an invention only its form, and are generally seen as weaker
        - Software: area of on-going controversy; Google vs Oracle; given to rise of "patent trolls"
    - **Copyright**: exclusive use of artistic, musical or literary works which prevents unauthorized duplication, distribution or modification
    - **Licensing**: a contract between the software producer and the consumer which limits the use and/or distribution of the software
    - **Trade Secrets**: intellectual property that is critical to a business, and significant damage would result if it were disclosed to competitors or the public
- **Import / Export controls**:
    - Every country has laws around the import and export of hardware and software. For example, the US has restrictions around the export of cryptographic technology, and Russia requires a license to import encryption technologies manufactured outside the country
- **Transborder data flow**:
    - Organizations should adhere to origin country-specific laws and regulations, regardless of where data resides
    - Also be aware of applicable laws where data is stored and systems are used
- **Privacy**:
    - Many laws include privacy protections for personal data. The EU's GDPR has strong privacy rules that apply to any organization anywhere that stores or processes the personal data of EU residents; these individuals must be told how their data is collected and used, and they must be able to opt out
    - The privacy guidelines of the **Organization for Economic Co-operation and Development (OECD)** require organizations to avoid unjustified obstacles to trans-border data flow, set limits to personal data

collection, protect personal data with reasonable security and more
    - Fourth Amendment to the US Constitution: the right of the people to be secure in their persons, houses, papers, effects against unreasonable search and seizure
    - Electronic Communication Privacy Act (ACPE): makes it a crime to invate electronic privacy of an individual, broadened the Federal Wiretap Act
    - HIPAA
    - HITECH
    - California SB 1386 (2002): immediate disclosure to individuals for PII breach
    - California Consumer Privacy Act (CCPA)
    - Children's Online Privacy Protection Act (COPPA) of 1998
    - GLBA
    - US Patriot Act of 2002
    - Family Education Rights and Privacy Act (FERPA): Grants privacy rights to students over 18, and the parents of minor students
    - EU's Data Protection Directive (DPD)
    - EU's General Data Protection Regulation (GDPR): key provisions
        - lawfulness, fairness, and transparency
        - purpose limitation
        - data minimization
        - accuracy
        - storage limitation
        - security
        - accountability
    - The EU-US **Privacy Shield** (formerly the EU-US Safe Harbor agreement) controls data flow from the EU to the United States. The EU has more stringent privacy protections and without the Privacy Shield, personal data flow from the EU to the United States would not be allowed

1.6 **Understand requirements for investigation types (i.e. administrative, criminal, civil, regulatory, industry standards)** An investigation will vary based on incident type. As an example, for a financial services company, a financial system compromise might cause a regulatory investigation. A system breach or website compromise might cause a criminal investigation. Each type of investigation has special considerations:

- **Administrative**: An administrative investigation has a primary purpose of providing the appropriate authorities with incident information. Thereafter, the authorities will determine the proper action, if any. Administrative investigations are often tied to HR scenarios, such as when a manager has been accused of improprieties
- **Criminal**: A criminal investigation occurs when a crime has been committed and you are working with a law enforcement agency to convict the alleged perpetrator. In such a case, it is common to gather evidence for a court of law, and to share the evidence with the defense. Therefore, you need to gather and handle the information using methods that ensure the evidence can be used in court. Remember that in a criminal case, a suspect must be proven guilty beyond a reasonable doubt. This is more difficult than showing a preponderance of evidence, which is often the standard in a civil case
- **Civil**: In a civil case, one person or entity sues another. For example, one company might sue another for a trademark violation. A civil case is typically about monetary damages, and doesn't involve criminality. In a civil

case, a preponderance of evidence is required to secure a victory. This differs from criminal cases, where a suspect is innocent until proven guilty beyond a reasonable doubt

- **Industry Standards**: An industry standards investigation is intended to determine whether an organization is adhering to a specific industry standard or set of standards, such as logging and auditing failed logon attempts. Because industry standards represent well-understood and widely implemented best practices, many organizations try to adhere to them even when they are not required to do so in order to improve security, and reduce operational and other risks
- **Regulatory**: A regulatory investigation is conducted by a regulatory body, such as the Securities and Exchange Commission (SEC) or Financial Industry Regulatory Authority (FINRA), against an organization suspected of an infraction. In such cases, the organization is required to comply with the investigation, for example, by not hiding or destroying evidence.

1.7 **Develop, document, and implement security policy, standards, procedures and guidelines** The top tier of a formalized hierarchical organization security documentation is the security policy. A security policy is a document that defines the scope of security needed by the organization, and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protections. It defines the strategic security objectives, vision, and goals and outlines the security framework of the organization. **Acceptable User Policy**: the AUP is a commonly produced document that exists as part of the overall security documentation infrastructure. This policy defines a level of acceptable performance and expectation of behavior and activity. Failure to comply with the policy may result in job action warnings, penalties, or termination.

Security Standards, Baselines and Guidelines

Once the main security policies are set, the remaining security docuemntation can be crafted from these policies.

- **Policies**: these are high-level documents, usually written by the management team. Policies are mandatory. A policy might provide requirements, but not the steps for implementation
- **Standards**: more descriptive than policies, standards define compulsary requirements for the homogenous use of hardware, software, technology, and security controls, uniformly implemented throughout the organization
- **Baseline**: defines a minimum level of security that every system throughout the organization must meet. Baselines are usually system specific and refer to industry / government standards. As an example, a baseline for server builds would be a list of configuration areas that should be applied to every server that is built. A Group Policy Object (GPO) in a Windows network is sometimes used to comply with standards. Configuration management solutions can also help you establish baselines and spot configurations that are not in alignment
- **Guideline**: offers recommendations on how standards and baselines should be implemented & serves as an operational guide for security professionals and users. Guidelines are flexible, and can be customized for unique systems or conditions. They state which security mechanism should be deployed instead of prescribing a specific product or control. They are not complusory
- **Procedure** (or Standard Operating Procedure or SOP): detailed, step-by-step how-to doc that describes the exact actions necessary to implement a specific security mechanism, control, or solution

1.8 **Identify, analyze, and prioritize Business Continuity (BC) requirements**

Business Continuity Planning (BCP) involves assessing the risk to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur

BCP is used to maintain the continuous operation of a business in the event of an emergency, with a goal to implement a combination of policies, procedures, and processes Business Continuity requires a lot of planning and preparation. Actual implementation of business continuity processes occur quite infrequently. The primary facets of business continuity are:

- Resilience: (e.g. within a data center and between sites or data centers),
- Recovery: if a service becomes unavailable, you need to recover it as soon as possible, and
- Contingency: a last resort in case resilience and recovery prove ineffective

BCP vs DR:

- BCP activities are typically strategically focused at a high level and center themselves on business processes and operations
- DR plans tend to be more tactical and describe technical activities such as recovery sites, backups, and fault tolerance

The overall goal of BCP is to provide a quick, calm, and efficient response in the event of an emergency and to enhance a company's ability to recover from a distruptive event promptly

The BCP process has four main steps:

- **Project scope and planning**: Developing the project scope and plan starts with gaining support of the management team, making a business case (cost/benefit analysis, regulatory or compliance reasons,etc.) and gaining approval to move forward. Next, you need to form a team with representatives from the business as well as IT. Then you are ready to begin developing the plan. Start with a business continuity policy statement, then conduct a business impact analysis (see next item), and then develop the remaining components: preventive controls, relocation, the actual continuity plan, testing, training and maintenance

- **Business impact analysis (BIA)**:Identify the systems and services that the business relies on and assess the impacts that a disruption or outage would cause, including the impacts on business processes like accounts receivable and sales. You also need to figure out which systems and services you need to get things running again (think foundational IT services such as the network and directory, which many other systems rely on). Finally, prioritize the order in which critical systems and services are recovered or brought back online. As part of the BIA, establish:

    - **recovery time objectives (RTO)** (how long it takes to recover),
    - **recovery point objectives (RPO)** (the maximum tolerable data loss), and
    - **maximum tolerable downtime (MTD)**, along with the costs of downtime and recovery

- **Continuity planning**: The first two phases of the BCP process (project scope and planning and the business impact analysis) focus on determining how the BCP process will work and prioritizing the business assets that need to be protected against interruption. The next phase of BCP development, continuity planning, focuses on the development and implementation of a continuity strategy to minimize the impact realized risks might have on protected assets

    - There are two primary subtasks involved in continuity planning:

        - Strategy development

        - Provisions and processes

    - The goal of this process is to create a **continuity of operations plan** (COOP), which focuses on how an org will carry out critical business functions starting shortly after a disruption occurs and extending up to one month of sustained operations

- **Approval and implementation**:

    - BCP plan now needs sr. management buy-in (should be endorsed by the org's top exec)
    - BCP team should create an implementation schedule, and all personnel involed should receive training on the plan

The top priority of BCP and DRP is people. **Always prioritize people's safety.** Get people out of harm's way, and then address IT recovery and restoration issues

1.9 **Contribute to and enforce personnel security policies and procedures**

People are often considered the weakest element in any security solution. No matter what physical or logical controls are deployed, humans can discover ways of to avoid them, circumvent or subvert them, or disable them. Malicious actors are routinely targeting users with phishing and spear phishing campaigns, social engineering, and other types of attacks. Everybody is a target. And once attackers compromise an account, they can use that entry point to move around the network and elevate their privileges. However, people can also become a key security asset when they are properly trained and are motivated to protect not only themselves but the security of the organization as well.

The following strategies can reduce your risk:

- **Candidate screening and hiring**: To properly plan for security, you must have standards in place for job descriptions, job classification, work tasks, job responsibilities, prevention of collusion, candidate screening, background checks, security clearances, employment agreements, and nondisclosure agreements. Screening employment candidates thoroughly is a key part of the hiring process. Be sure to conduct a full background check that includes a criminal records check, job history verification, education verification, certification validation and confirmation of other accolades when possible. Additionally, all references should be contacted.

- **Employment agreements and policies**: An employment agreement specifies job duties, expectations, rate of pay, benefits and information about termination. Sometimes, such agreements are for a set period (for example, in a contract or short-term job). Employment agreements facilitate termination when needed for an underperforming employee. The more information and detail in an employment agreement, the less risk (risk of a wrongful termination lawsuit, for example) the company has during a termination proceeding. For example, a terminated employee might take a copy of their email with them without thinking of it as stealing, but they are less likely to do so if an employment agreement or another policy document clearly prohibits it.

- example employee agreements:

    - non-compete
    - codes of conduct such as an acceptable use policy (AUP), which defines what is and isn’t acceptable acitivty, practice, or use for company equipemnt and resources

    - nondisclosure agreement (NDA), which is a doc used to protect confidential information from being disclosed by a current or former employee

- **Onboarding, transfers and termination processes**:

    - onboarding: process of bringing a new employee into the organization
    - creating documented processes allowing the new employee to be intgrated quickly and consistently
    - transfer: an employee moves from one job to another, likely requiring adjusted account access to maintain appropriate least privilege
    - termination or offboarding: offboarding is the removal of an employee's identity from the IAM system, once that person has left the oranization; can also be an element used when an employee transfers into a new role
    - whether cordial or abrupt, the ex-employee should be escorted off the premises and not allowed to return

- **Vendor, consultant, contractor agreements and controls**

    - Organizations commonly outsource many IT functions, particularly data center hosting, contact-center support, and application development.
    - Info security policies and procedures must address outsourcing secuity and the use of service providers, vendors and consultants. Access control, document exchange and review, maintenance, on-site assessment, process and policy review, and Service Level Agreements (SLAs) are examples of outsourcing security considerations

- **Compliance policy requirements**:

    - Compliance is the act of confirming or adhering to rules, policies, regulations, standards, or requirements
    - On a personnel level, compliance is related to individual employees following company policies and procedures
    - Employees need to be trained on company standards as defined in the security policy and remain in compliance with any contractual obligations (e.g. with PCI DSS)
    - Compliacne is a form of administrative or managerial security control
    - Compliance enforcement is the application of sanctions or consequences for failing to follow policy, training, best practices, or regulations

- **Privacy policy requirements**:

    - Personally identifiable information (PII) about employees, partners, contractors, customers and other people should be stored in a secure way, accessible only to those who require the information to perform their jobs.
    - Organizations should maintain a documented privacy policy which outlines the type of data covered by the policy and who the policy applies to. Employees and contractors should be required to read and agree to the privacy policy upon hire and on a regular basis thereafter (such as annually)

1.10 **Understand and apply risk management concepts**

- Identify threats and vulnerabilities

    - **Threats**: any potential occurrence that many cause an undersirable or unwanted outome for a specific asset; they can be intentional or accidental; loosely think of a threat as a weapon that could cause harm to a target
    - **Vulnerability**: the weakness in an asset or absense or weakness of a safeguard or countermeasure; a flaw, limitation, error, frailty, or susceptibility to harm
    - Threats and vulnerabilities are related: a threat is possible when a vulnerability is present
        - Threats exploit vulnerabilities, which results in exposure. Exposure is risk, and risk is mitigated by safeguards. Safeguards protect assets that are endangered by threats.
        - **Threat Agent/Actors**: intentionally exploit vulnerabilities
        - **Threat Events**: accidential occurrences and intentinoal exploitations of vulnerabilities
        - **Threat Vectors**: AKA attack vector is the path or means by which an attack or attacker can gain access to a target in order to cause harm
        - **Exposure**: being susceptible to asset loss because of a threat; the potential for harm to occur; quantitative risk analysis value of **exposure factor (EF)** is derived from this concept
        - **Risk**: the possiblity or likelihood that a threat will exploit a vulnerability to cause harm to an asset and the severity of damage that could result; the > the potential harm, the > the risk;
- Risk assessment/analysis
    - risk is threat with a vulnerability
    - risk = threat * vulnerability (or probability of harm * severity of harm)
    - addressing either the threat or threat agent or vulnerability directly results in a reduction of risk (known as threat mitigation)
    - Threats exploit vulnerabilities, which results in exposure. Exposure is risk, and risk is mitigated by safeguards. Safeguards protect assets that are endangered by threats
    - All IT systems have risk. All organizations have risk. There is no way to elminiate 100% of all risks. Instead upper management must decide which risks are acceptable, and which are not. There are two primary risk-assessment methodologies:
        - **Quantitative Risk Analysis**: assigns real dollar figures to the loss of an asset and is based on mathematical calculations
        - **Qualitative Risk Analysis**: assigns subjective and intangible values to the loss of an asset and takes into account perspectives, feelings, intuition, preferences, ideas, and gut reactions
        - Most organizations employ a hybrid of both risk assessment methodologies
        - The goal of risk assessment is to identify risks (based on asset-threat parings) and rank them in order of criticality
- Risk response
    - **Risk Assessment**: used to identify the risks and set criticality priorities, and then risk response is used to determine the best defense for each identified risk
    - Possible responses to risk:
        - Mitigation or reduction
        - Assignment or transfer
        - Deterrence
        - Avoidance
        - Acceptance
        - Reject or ignore

- Risk response formulation of a plan for each identified risk. For a given risk, a choice can be made to reduce the risk (risk mitigation), assign the risk to team for action (risk assignment), acceptance of the risk, or to ignore the risk (risk rejection)
- Countermeasure selection and implementation:
    - A **countermeasure**, sometimes referred to as a “control” or a “safeguard,” can help reduce risk
    - For exam preparation, understand how the concepts are integrated into your environment. This is not a step-by-step technical configuration, but the process of the implementation — where you start, in which order it occurs and how you finish
    - Keep in mind that security should be designed to support and enable business tasks and functions. Security controls, countermeasures, and safeguards can be implemented administratively, logically / technically, or physically. These 3 categories should be implemented in a conceptual layered defense-in-depth manner to provide maximum benefit. This is based on the concept that policies (part of administrative controls) drive all aspects of security and thus form the initial protection layer around assets. Then, logical and technical controls provide protection against logical attacks and exploits. Then, physical controls provide protection against real-world physical attacks against facilities and devices.
- Applicable Types of Controls
    - **Administrative**: the policies and procedures defined by an organization's security policy and other regulations or requirements
    - **Physical**:security mechanisms focused on providing protection to the facility and real world objects
    - **Preventive**: A preventive or preventative control is deployed to thwart or stop unwanted or unauthorized activity from occurring
    - **Deterrent**: A deterrent control is deployed to discourage security policy violations. Deterrent and preventative controls are similar, but deterrent controls often depend on individuals being convinced not to take an unwanted action
    - **Detective**: A detective control is deployed to discover or detect unwanted or unauthorized activity. Detective controls operate after the fact
    - **Compensating**: A compensating control is deployed to provide various options to other existing controls to aid in enforcement and support of security policies. They can be any controls used in addition to, or in place of, another control. They can be a means to improve the effectiveness of a primary control or as the alternative or failover option in the event of a primary control failure
    - **Corrective**: A corrective control modifies the environment to return systems to normal after an unwanted or unauthorized activity as occurred. It attempts to correct any problems resulting from a security incident
    - **Recovery**: An extension of corrective controls but have more advanced or complex abilities. A recovery control attempts to repair or restore resources, functions, and capabilities after a security policy violation. Recovery controls typically address more significant damaging events compared to corrective controls, especially when security violations may have occurred
    - **Directive**: A directive control is deployed to direct, confine, or control the actions of subjects to force or encourage compliance with security policies
- Control assessments (security and privacy)
    - Periodically assess security and privacy controls.What’s working, what isn’t? As part of this assessment, the existing documents must be thoroughly reviewed, and some of the controls must

be tested at random. A report is typically produced to show the outcomes and enable the organization to remediate deficiencies. Often, security and privacy control assessment are performed and/or validated by different teams, with the privacyteam handling the privacy aspects

- Monitoring and Measurement
  - Monitoring and measurement are closely aligned with identifying risks
  - While monitoring is used for more than security purposes, monitoring should be tuned to ensure the organization is notified about potential security incidents as soon as possible
  - If a security breach occurs, monitored systems and data become valuable from a forensics perspective. From the ability to derive root cause of an incident to making adjustments to minimize the chances of reoccurance
- Reporting
  - Risk Reporting is a key task to perform at the conclusion of risk analysis (i.e. production and presentation of a summarizing report)
  - A Risk Register or Risk Log is a document that inventories all identified risks to an organization or system or within an individual project. A risk register is used to record and track the activities of risk management, including:
    - identifying risks
    - evaluating the severity of, and prioritizing those risks
    - prescribing responses to reduce or eliminate the risks
    - track the progress of risk mitigation
- Continuous Improvement
  - Risk analysis is performed to provide upper management with the details necessary to decide which risks should be mitigated, which should be transferred, which should be deterred, which should be avoided, and which should be accepted
  - An **Enterprise Risk Management** (ERM) program can be evaluated using the **Risk Maturity Model (RMM)**. An RMM assesses the key indicators and activities of a mature, sustainable, and repeatable risk management process, typically relating the assessment of risk maturity against a five-level model such as:
    - **Ad hoc**: A chaotic starting point from which all organizations initiate risk management
    - **Preliminary**: Loose attempts are made to follow risk management processes, but each department may perform risk assessment uniquely
    - **Defined**: A common or standardized risk framework is adopted organization-wide
    - **Integrated**: Risk management operations are integrated into business processes, metrics are used to gather effectiveness data, and risk is considered an element in business strategy decisions
    - **Optimized**: Risk management focuses on achieving objectives rather than just reacting to external threats; increased strategic planning is geared toward business success rather than just avoiding incidents; and lessons learned are re-integrated into the risk management process.
- Risk Frameworks
  - A risk framework is a guide or recipe for how risk is to be accessed, resolved, and monitored
  - NIST established the **Risk Management Framework** (RMF) and the **Cybersecurity Framework** (CSF).The CSF is a set of guidelines for mitigating organizational cybersecurity risks, based on existing standards, guidelines, and practices

        - The RMF is intended as a risk management process to identify and respond to threats, and is defined in three core, interrelated Special Publications:
            - SP 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations
            - SP 800-39, Managing Information Security Risk
            - SP 800-30 Rev 1, Guide for Conducting Risk Assessments
            - The **RMF 7 steps**, and has **six cyclical phases**:
                - **Prepare** to execute the RMF from an organization and system-level perspective by establishing a context and priorities for managing security and privacy risk
                - **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss
                - **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk
                - **Implement** the controls and describe how the controls are employed within the system and its environment of operation
                - **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements
                - **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, and other organizations, and the nation is acceptable.
                - **Monitor** the system and associated controls on an on-going basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analysis, and reporting the security and privacy posture of the system
        - See my overview article, The NIST Risk Management Framework (https://blog.balancedsec.com/p/the-nist-risk-management-framework)
    - There are other risk frameworks, such as the British Standard BS 31100. Be familiar with frameworks and their goals

1.11 **Understand and apply threat modeling concepts and methodologies**

- **Threat Modeling**: security process where potential threats are identified, categorized, and analyzed. It can be performed as a proactive measure during design and development or as an reactive measure once a product has been deployed. Threat modeling identifies the potential harm, the probability of occurrence, the priority of concern, and the means to eradicate or reduce the threat
- Microsoft uses the **Security Development Lifecycle** (SDL) with the motto: "Secure by design, secure by default, secure in deployment and communication." It has two objectives:
    - Reduce the number of security-related design and coding defects
    - Reduce the severity of any remaining defects
- A defensive approach to threat modeling takes place during the early stages of development; the method is based on predicting threats and designing in specific defenses during the coding and crafting process. Security solutions are more cost effective in this phase than later. This concept should be considered a proactive approach to threat management

- Microsoft developed the **STRIDE threat model**:
    - Spoofing: an attack with the goal of gaining access to a target system through the use of falsified identity
    - Tampering: any action resulting in unauthorized changes or manipulation of data, whether in transit or in storage
    - Repudiation: the ability of a user or attacker to deny having performed an action or activity by maintaining plausible deniability
    - Information Disclosure: the revelation or distribution of private, confidential, or controlled information to external or unauthorized entities
    - Denial of Service (DoS): an attack that attempts to prevent authorized use of a resource. This can be done through flaw exploitation, connection overloading, or traffic flooding
    - Elevation of privilege: an attack where a limited user account is transformed into an account with greater privileges, powers, and access
- **Process for Attack Simulation and Threat Analysis (PASTA)** is a seven-stage threat modeling methodology. The seven steps of PASTA:
    - Stage I: Definition of the Objectives (DO) for the Analysis of Risk.
    - Stage II: Definition of the Technical Scope (DTS)
    - Stage III: Application Decomposition and Analysis (ADA)
    - Stage IV: Threat Analysis (TA)
    - Stage V: Weakness and Vulnerability Analysis (WVA)
    - Stage VI: Attack Modeling and Simulation (AMS)
    - Stage VII: Risk Analysis and Management (RAM)
- Each stage of PASTA has a specific list of objectives to achieve and deliverables to produce in order to complete the stage
- **Visual, Agile, and Simple Threat (VAST)** is a threat modeling concept that integrates threat and risk management into an Agile programming environment on a scalable basis
- Part of the job of the security team is to identify threats, using different methods:
    - Focus on attackers: this is a useful method in specific situations. For example, suppose that a developer's employment is terminated. After extracting data from the developer's computer, a determination is made that the person was disgruntled and angry. Understanding this situation as a possible threat, allows mitigation steps to be taken
    - Focus on assets: an organization's most valuable assets are likely to be targeted by attackers
    - Focus on software: organizations that develop applications in house, and can be viewed as part of the threat landscape. The goal isn't to identify every possible attack, but instead to focus on the big picture, identifying risks and attack vectors
- Understanding threats to the organization allow the documentation of potential attack vectors. Diagramming can be used to list various technologies under threat

1.12 Apply Supply Chain Risk Management (SRM) concepts

- Risks associated with hardware, software, and services
    - **Supply Chain Risk Management (SCRM)** is the means to ensure that all of the vendors or links in the supply chain are:
        - reliable,
        - trustworthy,

        - reputable organizations that disclose their practices and security requirements to their business partners (not necessarily to the public)
    - Each link in the chain should be responsible and accountable to the next link in the chain. Each handoff is properly organized, documented, managed, and audited. The goal of a secure supply chain is to ensure that the finished product is of sufficient quality, meets performance and operational goals, and provides stated security mechanisms, and that at no point in the process was any element counterfeited or subject to unauthorized or malicious manipulation or sabotage
- The supply chain can be a threat vector, where materials, software, hardware, or data is being obtained from a supposedly trusted source but the supply chain behind the source could have been compromised and asset poisoned or modified
- Third-party assessment and monitoring
    - Before doing business with another company, an organization needs to perform due-dilligence, and third-party assessments can help gather information and perform the assessment
    - An on-site assessment is useful to gain information about physical security and operations. During the document review, your goal is to thoroughly review all the architecture, designs, implementations, policies, procedures, etc. A good understanding of the current state of the environment, especially to understand any shortcomings or compliance issues prior to integrating the IT infrastructures. The level of access and depth of information obtained is usually proportional to how closely the companies will work together
- Minimum security requirements
    - As part of assessment, the minimum security requirements must be established. In some cases, the minimum security requirements are your company's security requirements. In other cases, new minimum security requirements need to be established. In such scenarios, the minimum security requirements should have a defined period
- Service-level requirements
    - A final area to review involves **Service Level Agreements (SLAs)**. Companies have SLAs for internal operations (such as how long it takes for the helpdesk to respond to a new ticket), for customers (such as the availability of a public-facing service) and for partner organizations (such as how much support a vendor provides a partner). All the SLAs should be reviewed. A company sometimes has an SLA standard that should be applied, when possible, to the service level agreements as part of working with another company. This can sometimes take time, as the acquiring company might have to support established SLAs until they expire or are up for renewal

1.13 **Establish and maintain a security awareness, education, and training program**

- Methods and techniques to present awareness and training
    - Before actual training can take place, awareness of security as a recognized entity must be created for users. Once this is accomplished, training, or teaching employees to perform their work tasks and to comply with the security policy can begin. All new employees require some level of training so that they will be able to comply with all standards, guidelines, and procedures mandated by the security policy. Education is a more detailed endeavor in which students/users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification or seeking job promotion.
    - Employees need to understand what to be aware of (types of threats, such as phishing and free USB sticks), how to perform their jobs securely (encrypt sensitive data, physically protect valuable assets) and

how security plays a role in the big picture (company reputation, profits,and losses). Training should be mandatory and provided both to new employees and yearly (at a minimum) for ongoing training. Routine tests of operational security should be performed (such as phishing test campaigns,tailgating at company doors and social engineering tests)

        - Social engineering. While many organizations don't perform social engineering campaigns (testing employees using benign social engineering attempts) as part of security awareness, it is likely to gain traction. Outside of campaigns, presenting social engineering scenarios and information is a common way to educate
        - Phishing. Phishing campaigns are very popular. Many organizations use third-party services to routinely test their employees with fake phishing emails. Such campaigns produce valuable data, such as the percentage of employees who open the phishing email, the percentage who open attachments or clicklinks, and the percentage who report the fake phishing email as malicious
        - Security champions. The term "champion" has been gaining ground. Organizations often use it to designate a person on a team who is a subject matter expert in a particular area or responsible for a specific area. For example, somebody on your team could be a monitoring champion — they have deep knowledge around monitoring and evangelize the benefits of monitoring to the team or other teams. A security champion is a person responsible for evangelizing security, helping bring security to areas that require attention, and helping the team enhance their skills
        - Gamification. Legacy training and education are typically based on reading and then answering multiple-choice questions to prove one's knowledge. Gamification aims to make training and education more fun and engaging by packing educational material into a game. That might mean playing an actual game, but it might also mean keeping track of scores, having leader boards, and enabling people to earn somethingbased on their scores or progress (kudos, special avatars or similar). Gamification has enabled organizations to get more out of the typical employee training
    - Periodic content reviews
        - Threats are complex, so training needs to be relevant and interesting to be effective. This means updating training materials and changing out the ways which security is tested and measured. If you always use the same phishing test campaign or send it from the same account on the same day, it isn't effective. The same applies to other materials. Instead of relying on long and detailed security documentation for training and awareness, consider using internal social media tools, videos and interactive campaigns
    - Program effectiveness evaluation
        - Time and money must be allocated for evaluating the company's security awareness and training. The company should track key metrics, such as the percentage of employees who click on a fake phishing campaign email link. Is the awareness and training bringing that number clicks down over time? If not, re-evaluation may be needed

Also see my articles on risk management:

- Part 1 (https://blog.balancedsec.com/p/risk-concepts-from-the-cissp-part-1) introduces risk and risk terminology from the lens of the (ISC)² Official Study Guide
- Since the primary goal of risk management is to identify potential threats against an organizaton's assets, and bring those risks into alignment with an organization's risk appetite, in Part2 (https://blog.balancedsec.com/p/risk-concepts-from-the-cissp-part-2), we cover the threat assessment -- a process of examining and evaluating cyber

threat sources with potential system vulnerabilities.We look at how a risk assessment helps drive our understanding of risk by pairing assets and their associated potential threats, ranking them by criticality. We also discussed quantitative analytic tools to help provide specific numbers for various potential risks, losses, and costs

- In the third installment (https://blog.balancedsec.com/p/risk-concepts-from-the-cissp-part-3), we review the outcome of the risk assessment process, looking at total risk, allowing us to determine our response to each risk/threat pair and perform a cost/benefit review of a particular safeguard or control. We also look at the categories and types of controls and the idea of layering them to provide several different types of protection mechanisms. We also review the important step of reporting out our risk analysis and recommended responses, noting differences in requirements for messaging by group.

Domain 2 **Asset Security**

Domain 2 of the CISSP exam covers asset security making up ~10% of the test. Asset security includes the concepts, principles, and standards of monitoring and securing any asset important to the organization.

The Asset Security domain focuses on collecting, handling, and protecting information throughout its lifecycle. The first step is classifying information based on its value to the organization

2.1 Identify and classify information assets

Data Classification

- Managing the data lifecycle refers to protecting it from cradle to grave -- steps need to be taken to protect data when its first created until it's destroyed
- One of the first steps in the lifecycle is identifying and classifying information and assets, often within a security policy
- In this context, assets include sensitive data, the hardware used to process that data, and the media used to store/hold it
- Sensitive data is any information that isn't public or unclassified, and can include anything an organization needs to protect due to its value, or to comply with existing laws and regulations
- **Personally Identifiable Information (PII)** (NIST SP 800-122 (https://csrc.nist.gov/publications/detail/sp/800-122/final) provides formal definitions), and **Protected Health Information (PHI)** are two important types to protect
- **Proprietary data**: any data that helps an organization maintain a competitive edge
- Organizations classify data using labels
    - government classification labels include:
        - Top Secret: if disclosed, could cause massive damage to national security, such as the disclosure of spy satellite information
        - Secret: if disclosed, can adversely affect national security
        - Unclassified: not sensitive
    - non-government organizations use labels such as:
        - Confidential/Proprietary: only used within the organization and, in the case of unauthorized disclosure, it could suffer serious consequences
        - Private: may include personal information, such as credit card data and bank accounts. Unauthorized disclosure can be disastrous
        - Sensitive: needs extraordinary precautions to ensure confidentiality and integrity

        - Public: can be viewed by the general public and, therefore, the disclosure of this data would not cause damage
    - labels can be as granular and custom as required by the organization
- It is important to protect data in all states: at rest, in transit, or in use
- The best way to protect data confidentiality is via use of strong encryption

Asset Classification

- It's important to identify and classify assets, such as systems, mobile devices etc.
- Asset classifications should match data classification - i.e. if a computer is processing top secret data, the computer should be classified as a top secret asset
- **Clearance**: relates to access to certain classfication of data or equipment, and who has access to that level or classification
- A **formal access approval process** should be used to change user access; the process should involve approval from the data/asset owner, and the user should be informed about rules and limits
    - before a user is granted access they should be educated on working with that level of classification
- Classification levels can be used by businesses during acquisitions, ensuring only personnel who need to know are involved in the assessment or transition

In general, classification labels help users use data and assets properly, for instance by restricting dissemination or use of assets by their classification

2.2 Establish information and asset handling requirements

- The data and asset handling key goal is to prevent data breaches, by using:
    - **Data Maintenance**: on-going efforts to organize and care for data through it's life cycle
    - **Data Loss Prevention (DLP)**: systems that detect and block data exfiltration attempts; two primary types:
        - Network-Based DLP
        - Endpoint-Based DLP
- **Marking**: (AKA labeling) sensitive information/assets ensures proper handling (both physically and electronically)
- **Handling**: refers to secure transport of media through its lifetime
- **Data Collection Limitation**: prevent loss by not collecting unnecessary sensitive data
- **Data Location**: keep dup copies of backups, on- and off-site
- **Storage**: define storage locations and procedures by storage type; use physical locks for paper-based media, and encrypt electronic data
- **Destruction**: destroy data no longer needed by the organization; policy should define acceptable destruction methods by type and classification (see NIST SP-800-88 for details (https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final))
    - **Erasing**: usually refers to a delete operation on media, leaving data remanence
    - **Clearing**: over-writing existing data
    - **Purging**: usually refers to mutliple clearing passes combined with other tools (see below) -- not considered acceptable for top secret data
- **Data Remanence**: data remaining on media after typical erasure; to ensure all remanence is removed, the following tools can help:
    - **Degaussing**: used on magentic media

- **(Physical) destruction**: used for SSD/electronic components, or in combination with other less-secure methods
- **Cryptographic Erasure**: AKA cryptoshedding, basically destroying encryption key; may be only secure method for cloud storage

2.3 Provision resources securely

- The primary purpose of security operations practices is to safeguard assets such as information, systems, devices, facilities, and apps; these practices help to identify threats, vulnerabilities, and implement controls to reduce the risk to these asssets
- Implementing common security operations concepts, along with performing periodic security audits and reviews demonstrates a level of due care
- **need-to-know** principle imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks
- **least privilege** principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more

Information and Asset Ownership

- **Data owner**: the person who has ultimate organizational responsibility for data; usually sr. manager (CEO,president, dept. head); data owners typically delegate data protection tasks to others in the org

Asset Inventory

- Software assets are operating systems and applications; software licensing also refers to ensuring that systems do not have unauthorized software installed
- To protect intangible inventories (like intellectual property, patents, trademarks, and company's reputation, and copyrights), they need to be tracked

2.4 Manage data lifecycle

Data roles

- The **system owner** controls the computer storing the data. Usually includes software and hardware configurations and support services (e.g. cloud implementation). System owner is responsible for system operation and maintenance, and associated updating/patching as well as related procurement activities
- The **data custodian** is responsible for the protection of data through maintenance activities, backing up and archiving, and preventing the loss or corruption and recovering data
- The **security administrator** is responsible for ensuring the overall security of the entire infrastructure; they perform tasks that lead to the discovery of vulnerabilities, monitor network traffic and configure tools to protect the network (like firewalls and antivirus software). They also devise security policies, plans for business continuity and disaster recovery and train staff
- **Supervisors** are responsible for overseeing the activities of all the above entities and all support personnel. They ensure team activities are conducted smoothly and that personnel is properly skilled for the tasks assigned
- **Users** must comply with rules, mandatory policies, standards and procedures. Users have access to data according to their roles and their need to access information

Data Collection

- One of the easiest ways of preventing the loss of data is to simply not collect it
- The guideline: if the data doesn't have a clear purpose for use, don't collect it, and don't store it; this is why many privacy regulations mention limiting data collection

Data Location

- **Data location** in this context, refers to the location of data backups or data copies
- If a company's system is on-prem, keeps data on-site, but regularly backups up data, best practice is to keep a backup copy on site and backup copy off-site
- Consider distance between data/storage locations to mitigate potential mutual (primary and backup) damage risk

Data Maintenance and Retention

- **Data maintenance** refers to managing data as through the data lifecycle (creation, usage, retirement). Data maintenance is the process (often automated) of making sure the data is available (or not available) based on where it is in the lifecycle
- Ensuring appropriate asset protection requires that sensitive data be preserved for a period of not less than what is business-required, but for no longer than necessary
- Encrypt sensitive data
- Safeguard assets via basic security controls to enforce appropriate levels of confidentiality, integrity and availability and act per security policies, standards, procedures and guidelines
- Retention requirements apply to data or records, media holding sensitive data, systems that process sensitive data, and personnel who have access to sensitive data
- Three fundamental retention policy questions:
    - **How to retain**: data should be kept in a manner that makes it accessible whenever required; take taxonomy (or the scheme for data classification) into account
    - **How long to retain data**: general guidelines for business data is 7 years (but can vary by country/region/regulation)
    - **What data** to retain

Data Destruction

- Destroy sensitive data when it is no longer needed
- An organization's security or data policy should define the acceptable methods of destroying data based on the data's classification
- Note again: even when using manufacturers SSD wiping tools, data can remain, and therefore the best SSD wipe method is destruction

2.5 Ensure appropriate asset retention (e.g. EOL, EOS)

- Hardware: even if you maintain data for the appropriate retention period, it won't do you any good if you don't have hardware that can read the data

- Personnel: beyond retaining data for required time periods and maintaining hardware to read the data, you need personnel who know how to operate the hardware to execute restoraton processes

- End-Of-Life (EOL): often identified by vendors as the time when they stop offering a product for sale
- End-Of-Support (EOS)/End-Of-Service-Life (EOSL): often used to identify when support ends for a product
- EOL,EOS/EOSL can apply to either software or hardware

2.6 Determine data security controls and compliance requirements

You need security controls that protect data in each possible state: at rest, in transit or in use.

Each state requires a different approach to security. There aren't as many security options for data in use as there are for data at rest or data in transit. Keeping the systems patched, maintaining a standard computer build process, and running anti-virus/malware are typically the real-world primary protections for data in use

The three data states are at rest, in transit, and in use

- **Data at rest**: any data stored on media such as hard drives or external media
- **Data in transit**: any data transmitted over a network
- Encryption methods protect data at rest and in transit
- **Data in use** refers to data in memory and used by an application
- Applications should flush memory buffers to remove data after it is no longer needed

Scoping and Tailoring

After selecting a control baseline, orgs fine-tune with tailoring and scoping processes. A big part of the tailoring process is aligning controls with an organization's specific security requirements

- **Tailoring:** refers to modifying the list of security controls within a baseline to align with the organization's mission
    - includes the following activities:
        - Identifying and designating common controls
        - Applying scoping considerations
        - Selecting compensating controls
        - Assigning control values
- **Scoping**: part of the tailoring process and refers to reviewing a list of baseline security controls and selecting only those controls that apply to the systems you're trying to protect
    - Scoping processes eliminate controls that are recommended in a baseline

Standards Selection

- Organizations need to identify the standards (e.g. PCI DSS, GDPR etc) that apply and ensure that the security controls they select fully comply with these standards
- Even if the organization doesn't have to comply with a specific standard, using a well-designed community standard can be helpful (e.g. NIST SP 800 documents)
- **Standards selection** is the process by which organizations plan, choose and document technologies or architectures for implementation. (For example, you might evaluate three vendors for a security control; you could use a standards selection process to help determine which solution best fits the organization)
- Vendor selection is closely related to standards selection but focuses on the vendors, not the technologies or solutions

The overall goal is to have an objective and measurable selection process. If you repeat the process with a totally different team, the alternate team should come up with the same selection

Data Protection Methods

Data protection methods include:

- **digital rights management (DRM)**: methods used in attempt to protect copyrighted materials
- **Cloud Access Security Brokers (CASBs)** - software placed logically between users and cloud based resources, that can ensure that cloud resources have the same protections as resources within a network.

Note that Entities must comply with the EU GDPR, use additional data protection methods such as pseudonymization, tokenization, and anonymization

Options for protecting your data vary depending on its state:

- Data at rest:consider encryption for operating system volumes and data volumes, and backups as well. Be sure to consider all locations for data at rest, such as tapes, USB drives, external drives, RAID arrays, SAN, NAS, and optical media.
    - DRM is useful for data at rest because DRM "travels with the data" regardless of the data state. DRM is especially useful when you can't encrypt data volumes
    - A CASB solution often combines DLP, a web application firewall with some type of authentication and authorization, and a network firewall in a single solution. A CASB solution is helpful for protecting data in use (and data in transit)
- Data in transit: think of data in transit wholistically -- moving data from anywhere to anywhere. You can use encryption for data in transit.
    - Example: a web server uses a certificate to encrypt data being viewed by a user, or IPsec encrypting a communication session. There are many options. The most important point is to use encryption whenever possible, including for internal-only web apps
    - DLP solutions are useful for data in transit, scanning data on the wire, and stopping the transmission/transfer,based on the DLP rules set (e.g. outbound data that contains numbers matching a social security number pattern, a DLP rule can be used to block that traffic)

Domain 3 **Security Architecture and Engineering**

You may find this domain to be more technical than others, and if you have experience woring in a security engineering role you likely have an advantage. If not, allocate extra time to this domain to ensure you have a good understanding of the topics

3.1 Research, implement, and manage engineering processes using secure design principles

- **Threat modeling**: a security process where potential threats are identified, categorized, and analyzed. It can be performed as a proactive measure during design and development or as an reactive measure once a product has been deployed

    - Threat modeling identifies the potential harm, the probability of occurrence, the priority of concern, and the means to eradicate or reduce the threat

- **Least privilege**: states that subjects are granted only the privileges necessary to perform assigned work tasks and no more; this concept extends to data and systems

    - Limiting and controlling privileges based on this concept protects confidentiality and data integrity

- **Defense in Depth**: AKA layering, is the use of multiple controls in a series, where a single failed control should not result in exposure of systems or data. Layers should be used in a series (one after the other), NOT in parallel. When you see the terms levels, multilevel, layers, classifications, zones, realms, compartments, protection rings etc think about Defense in Depth

- **Secure defaults**: when you think about defaults, consider how something operates brand new, just turned over to you by the vendor

    - e.g. wireless router default admin password, or firewall configuration requiring changes to meet an organization's needs

- **Fail securely**: if a system, asset, or process fails, it shouldn't reveal sensitive information, or be less secure than during normal operation. Failing securely could involve reverting to defaults

- **Separation of duties (SoD)**: separation of duties (SoD) and responsibilities ensures that no single person has total control over a critical function or system; SoD is a process to minimize opportunities for misuse of data or environment damage.

    - e.g. one person sells tickets, another collects tickets and restricts access to ticket holders in a movie theater

- **Keep it simple**: AKA keep it simple, stupid (KISS), this concept is the encouragement to avoid overcomplicating the environment, organization, or product design

- **Zero Trust**: "assume breach"; a security concept and alternative the traditional (castle/moat) approach where nothing is automatically trusted. Instead each request for activity or access is assumed to be from an unknown and untrusted location until otherwise verified;

    - Goal is to have every access request authenticated, authorized, and encrypted prior to access being granted to an asset or resource
    - See my article on an Overview of Zero Trust Basics (https://blog.balancedsec.com/p/an-overview-of-zero-trust-basics)

- **Privacy by design (PbD)**: a guideline to integrate privacy protections into products during the earliest design phase rather than tacking it on at the end of development;

    - Same overall concept as "security by design" or "integrated security" where security is an element of design and architecture of a product starting at initiation and continuing through the software development lifecycle (SDLC)
    - There are 7 recognized principles to achieve privacy by design:

        - Proactive, preventative: think ahead and design for things that you anticipate might happen
        - Default setting: make private by default, e.g. social media app shouldn't share user data with everybody by default
        - Embedded: build privacy in; don’t add it later
        - Full functionality, positive-sum: achieve both security and privacy, not just one or the other
        - Full lifecycle protection: privacy should be achieved before, during and after a transaction. Part of this is securely disposing of data when it is no longer needed
        - Visibility, transparency, open: publish the requirements and goals; audit them and publish the findings
        - Respect, user-centric: involve end users, providing the right amount of information for them to make informed decisions about their data

- **Trust but verify**: based on a Russian proverb, and no longer sufficient; it's the traditional approach of trusting subjects and devices within a company's security perimeter automatically, leaving an org vulnerable to insider attacks and providing intruders the ability to easily perform lateral movement

- **Shared responsibility**: the security design principle that indicates that organizations do not operate in isolation

    - Everyone in an organization has some level of security responsibility
    - the job of the CISO and security team is to establish & maintain security
    - The job of regular employees to perform their tasks within the confines of security
    - The job of the auditor is to monitor the environment for violations
    - When working with third parties, especially with cloud providers, each entity needs to understand their portion of the shared responsibility of performing work operations and maintaining security. This is often referenced as the **cloud shared responsibility model**

3.2 Understand the fundamental concepts of security modles (e.g. Biba, Star Model, Bell-LaPadula)

Security models:

- Intended to provide an explicit set of rules that a computer can follow to implement the fundamental security concepts, processes, and procedures of a security policy
- Provide a way for a designer to map abstract statements into a security policy prescribing the algorithms and data structures necessary to build hardware and software
- Enable people to access only the data classified for their clearance level
- **Bell-LaPadula**: Model was established in 1973. The goal is to ensure that information is exposed only to those with the right level of classification
    - Focuse is on confidentiality
    - Simple property: No read-up
    - Star (*) property: No write-down (AKA confinement property)
    - Discretionary Security Property: uses an access matrix (need to know in order to access)
    - Doesn't address covert channels
- **Biba**: Released in 1977, this model was created to supplement Bell-LaPadula
    - Focus is on integrity
    - “No read down” (for example, users with a Top Secret clearance can’t read data classified as Secret)
    - “No write up” (for example, a user with a Secret clearance can’t write data to files classified as Top Secret)

    - By combining it with Bell-LaPadula, you get both confidentiality and integrity
- **Take-Grant**:
    - The take-grant model employs a directed graph to dictate how rights can be passed from one subject to another, or from a subject to an object
    - Four rules:
        - take
        - grant
        - create
        - remove
- **Clark-Wilson**:
    - Designed to protect integrity using the access control triplet
    - A program interface is used to limit what is done by a subject; if the focus of an intermediary program between subject and object is to protect integrity, then it is an implementation of the Clark-Wilson model
- **Brewer and Nash Model**:
    - AKA "ethical wall", and "cone of silence"
    - created to permit access controls to change dynamically based on a user's previous activity
- **Goguen-Meseguer Model**:
    - An integrity model
    - Foundation of noninterference conceptual theories
- **Sutherland Model**:
    - Focuses on preventing interference in support of integrity
- **Graham-Denning Model**
    - Focused on the secure creation and deletion of both subjects and objects
    - 8 primary protection rules or actions
        - 1-4:securely create/delete a subject/object
        - 5-8:securely provide the read/grant/delete/transfer access right
- **Harrison-Ruzzo-Ullman Model**:
    - Focuses on the assignment of object access rights to subjects as well as the resilience of those assigned rights
    - HRU is an extension of Graham-Denning model
- **Star Model**:
    - Not an official model, but name refers to using asterisks (stars) to dictate whether a person at a specific level of confidentiality is allowed to write data to a lower level of confidentiality
    - Also determines whether a person can read or write to a higher or lower level of confidentiality

3.3 Select controls based upon systems security requirements

Be familiar with the **Common Criteria (CC)** for Information Technology Security Evaluation

- The CC provides a standard to evaluate systems, defining various levels of testing and confirmation of systems' security capabilities
- The number of the level indicates what kind of testing and confirmation has been performed
- The important concepts:
    - To perform an evaluation, you need to select the **Target of Evaluation (TOE)** (e.g. firewall or an anti-malware app)

    - The evaluation process will look at the **protection profile (PP)**, which is a document that outlines the security needs (customer "I wants"). A vendor might use a specific protection profile for a particular solution
    - The evaluation process will look at the **Security Target (ST)**, specifying the claims of security from the vendor that are built into a TOE (the ST is usually published to customers and partners and available to internal staff)
    - An organization's PP is compared to various STs from the selected vendor's TOEs, and the closest or best match is what the org purchases
    - The evaluation will attempt to gauge the confidence level of a security feature
    - **Security assurance requirements (SARs)** are documented and based on the development of the solution
    - Key actions during development and testing should be captured
    - An **evaluation assurance level (EAL)** is a numerical rating used to assess the rigor of an evaluation. The scale is EAL 1 (cheap and easy) to EAL7 (expensive and complex)
        - 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, designed, and tested
        - EAL7: formally verified, designed, and tested
- **Authorization to Operate (ATO)**: official auth to use specific IT systems to perform tasks/accept identified risks

3.4 Understand security capabilities of Information Systems (IS) (e.g. memory protection, Trusted Platform Model (TPM), encryption/decryption)

Security capabilities of information systems include memory protection, virtualization, Trusted Platform Module (TPM), encryption/decryption, interfaces, and fault tolerance

A computing device is likely running multiple applications and services simultaneously, each occupying a segment of memory. The goal of memory protection is to prevent one application or service from impacting another. There are two primary memory protection methods:

- Process isolation: OS provides separate memory spaces for each processes instructions and data, and prevents one process from impacting another
- Hardware segmentation: forces separation via physical hardward controls rather than logical processes; in this type of segmentation, the operating system maps processes to dedicated memory locations

Virtualization: technology used to host one or more operating systems within the memory of a single host, or to run applications that are not compatible with the host OS. The goal is to protect the hypervisor and ensure that compromising one VM doesn't affect others on that host

Trusted Platform Module (TPM): a cryptographic chip that is sometimes included with a client computer or server. A TPM enhances the capabilities of a computer by offering hardware-based cryptographic operations. Many security products and encryption solutions require a TPM

- TPM is both a specification for a cryptoprocessor chip on a motherboard and the general name for implementation of the specification
- A TPM is an example of a **hardware security module (HSM)**
- An HSM is a cryptoprocessor used to manage and store digital encryption keys, accelerate crypto operations, support faster digital signatures, and improve authentication

User interface: a constrained UI can be used in an application to restrict what users can do or see based on their privileges

- e.g. dimming/graying out capabilities for users without the correct privilege

An interface is also the method by which two or more systems communicate Be aware of the common security capabilities of interfaces:

- Encryption/decryption: when communications are encrypted, a client and server can communicate without exposing information to the network; when an interface doesn't provide such a capability, use IPsec or another encrypted transport mechanism
- Signing: used for non-repudiation; in a high-security environment, both encrypt and sign all communications if possible

Fault tolerance: capability used to enhance availability. In the event of an attack (e.g. DoS), or system failure, fault tolerance helps keep a system up and running

3.5 Assess and mitigate the vulnerabilities of security architectures, designs and solution elements

This objective relates to identifying vulnerabilities and corresponding mitigating contols and solutions. The key is understanding the types of vulnerabilities commonly present in different environments, and their mitigation options

- **Client-based systems**: client computers are the most attacked entry point
    - Compromised client computers can be used to launch other attacks
    - Productivity software and browsers are constant targets
    - Even patched client computers are at risk due to phishing and social engineering vectors
    - Mitigation: run a full suite of security software, including anti-virus/malware, anti-spyware, and host-based firewall
- Server-based systems:
    - Data Flow Control: movement of data between processes, between devices, across a network, or over a communications channel
    - Management of data flow seeks to minimize latency/delays, keep traffic confidential (i.e. using encryption), not overload traffic (i.e. load balancer), and can be provided by network devices/applications & services
    - While attackers may initially target client computers, servers are often the goal
    - Mitigation: regular patching, deploying hardened server OS images for builds, and use host-based firewalls
- **Database systems**: databases often store a company's most sensitive data (e.g. proprietary, CC info, PHI, and PII)

    - Attackers may use inference or aggregation to obtain confidential information
    - **Aggregation attack**: process whereby SQL provides a number of functions that combine records from one or more tables to produce potentially useful info
    - **Inference attack** involves combining several pieces of nonsensitive info to gain access to that which should be classified at a higher level; inference makes use of the human mind's deductive capacity rather than the raw mathematical ability of database platforms

- **Cryptographic systems**: the goal of a well-implemented cryptographic system is to make compromise too time-consuming and/or expensive. Each component has vulnerabilities:

    - **Kerckhoff's Principle** (AKA Kerckhoff's assumption): a cryptographic system should be secure even if everything about the system, except the key, is public knowledge
    - Software: used to encrypt/decrypt data; can be a standalone app, command-line, built into the OS or called via API. Like any software, there are likely bugs/issues, so regular patching is important
    - Keys: dictate how encryption is applied through an algorithm. A key should remain secret, otherwise the security of the encrypted data is at risk
        - **Key space**:represents all possible permutations of a key
        - Key space best practices:
            - key length is an important consideration; use as long of a key as possible (your goal is to outpace projected increase in cryptanalytic capability during the time the data must be kept safe); longer keys discourage brute-force attacks
                - a 256-bit key is typically minimum recommendation for symmetric encryption
                - 2048-bit key typically the minimum for asymmetric
            - always store secret keys securely, and if you must transmit them over a network, do so in a manner that protects them from unauthorized disclosure
            - select the key using an approach that has as much randomness as possible, taking advantage of the entire key space
            - destroy keys securely, when no longer needed Always base key length on your requirements and sensitivity of the data being handled
    - Algorithms: choose algorithms (or ciphers) with a large key space and a large random **key value** (key value is used by an algorithm for the encryption process)
        - Algorithms themselves are not secret, but instead well-known with extensive public details about history and how they function

- **Industrial control systems (ICS)**: ICS is a form of computer-management device that controls industrial processes and machines, also known as operational technology (OT)

    - **Supervisory control and data acquisition (SCADA)**: systems used to control physical devices such as those found in an electrical power plant or factory. SCADA systems are well suited for distributed environments, such as those spanning continents
    - Some SCADA systems still rely on legacy or proprietary communications, which put them at risk, especially as attackers gain knowledge of such systems and their vulnerabilities
    - SCADA risk mitigations:
        - isolate networks
        - limit access physically and logically

        - restrict code to only essential apps
        - log all activity

- **Cloud-based systems**: on-demand access to computing resources available from almost anywhere
    - Cloud's primary challenge: resources are outside the org's direct control, making it more difficult to manage risk
    - Orgs should formally define requirements to store and process data stored in the cloud
    - Focus your efforts on areas that you can control, such as the network entry and exit points (i.e. firewalls and similar security solutions)
    - All sensitive data should be encrypted, both for network communication and data-at-rest
    - Use centralized identity access and management system, with multifactor authentication
    - Customers shouldn't use encryption controlled by the vendor, eliminating risks to vendor-based insider threats, and supporting destruction using
        - **cryptographic erase**: methods that permanently remove the cryptographic keys
    - Capture diagnostic and security data from cloud-based systems and store in your security information and event management (SIEM) system
    - Ensure that your cloud configuration matches or exceeds your on-premise security requirements
    - Understand the cloud vendor's security strategy
    - Cloud shared responsibility by model:
        - Software as a Service (SaaS):
            - the vendor is responsible for all maintenance of the SaaS services
        - Platform as a Service (PaaS):
            - customers deploy apps that they've created or acquired, manage their apps, and modify config settings on the host
            - the vendor is responsible for maintenance of the host and the underlying cloud infrastructure
        - Infrastructure as a Service (IaaS):
            - IaaS models provide basic computing resources to customers
            - customers install OSs and apps and perform required maintenance
            - the vendor maintains cloud-based infra, ensuring that customers have access to leased systems
- **Distributed systems distributed computing environment (DCE)**: a collection of individual systems that work together to support a resource or provide a service
    - DCEs are designed to support communication and coordination among their members in order to achieve a common function, goal, or operation

    - Most DCEs have duplicate or concurrent components, are asynchronous, and allow for fail-soft or independent failure of components
    - DCE is AKA concurrent computing, parallel computing, and distributed computing
    - DCE solutions are implemented as client-server, three-tier, multi-tier, and peer-to-peer
    - Securing distributed systems:
        - in distributed systems, integrity is sometimes a concern because data and software are spread across various systems, often in different locations
        - Client/server model network is AKA a distributed system or distributed architecture
            - security must be addressed everywhere instead of at a single centralized host
            - processing and storage are distributed on multiple clients and servers, and all must be secured
            - network links must be secured and protected

- **Internet of things (IoT)**: a class of smart devices that are internet-connected in order to provide automation, remote control, or AI processing to appliances or devices

    - An IoT device is almost always a separate/distinct hardware that is used on its own or in conjunction with an existing system
    - IoT security concerns often relate to access and encryption
    - IoT is often not designed with security as a core concept, resulting in security breaches; once an attacker has remote access to the device they may be able to pivot
    - Securing IoT:
        - Deploy a distinct network for IoT equipment, kept separate and isolated (known as **three dumb routers**)
        - Keep systems patched
        - Limit physical and logical access
        - Monitor activity
        - Implement firewalls and filtering
        - Never assume IoT defaults are good enough, evaluate settings and config options, and make changes to optimize security while supporting business function
        - Disable remote management and enable secure communication only (such as over HTTPS)
        - Review IoT vendor to understand their history with reported vulnerabilities, response time to vulnerabilities and their overall approach to security
        - Not all IoT devices are suitable for enterprise networks

- **Microservices**: a feature of web-based solutions and derivative of SOA

    - A microservice is simply one element, feature, capability, business logic, or function of a web application that can be called upon or used by other web applications
    - Microservices are usually small and focused on a single operation, designed with few dependencies, and are based on fast short-term development cycles (similar to Agile)
    - Securing microservices:
        - using HTTPS only
        - encrypt everything possible and use routine scanning

        - closely aligned with microservices is the concept of shifting left, or addressing security earlier in the SDLC; also integrating it into the CI/CD pipeline
        - consider the software supplychain or dependencies of libries used, when addressing updates and patching

- **Containerization**: AKA OS virtualization is based on the concept of eliminating the duplication of OS elements in a virtual machine; instead each application is placed into a container that includes only the actual resources needed to support the enclosed application, and the common or shared OS elements are then part of the hypervisor

    - Containerization is able to provide 10 to 100 x more application density per physical server compared to traditional virtualization
    - Vendors often have security benchmarks and hardening guidelines to follow to enhance container security
    - Securing containers:
        - container challenges include the lack of isolation compared to a traditional infrastructure of physical servers and VMs
        - scan container images to reveal software with vulnerabilities
        - secure your registries: use access controls to limit who can publish images, or even access the registry; require images to be signed
        - harden container deployment including the OS of the underlying host, using firewalls, and VPC rules, and use limited access accounts
        - reduce the attack surface by minimizing the number of components in each container, and update and scan them frequently

- **Serverless architecture** (AKA **function as a service (FaaS)**): a cloud computing concept where code is managed by the customer and the platform (i.e. supporting hardware and software) or servers are managed by the CSP

    - Applications developed on serverless architecture are similar to microservices, and each function is created to operate independently and automonomously
    - A serverless model, as in other CSP models, is a shared security model,and your organization and the CSP share security responsibility

- **Embedded systems**: any form of computing component added to an existing mechanical or electrical system for the purpose of providing automation, remote control, and/or monitoring; usually including a limited set of specific functions

    - Embedded systems can be a security risk because they are generally static, with admins having no way to update or address security vulnerabilities (or vendors are slow to patch)
    - Embedded systems focus on minimizing cost and extraneous features
    - Embedded systems are often in control of/associated with physical systems, and can have real-world impact
    - Securing embedded systems:
        - ebedded systems should be isolated from the internet, and from a private production network to minimize exposure to remote exploitation, remote control, and malware
        - use secure boot feature and physically protecting the hardware

- **High-performance computing (HPC)** systems: platforms designed to perform complex calculations/data manipulation at extremely high speeds (e.g. super computers or MPP); often used by large orgs, universities, or gov agencies
    - An HPC solution is composed of three main elements:
        - compute resources
        - network capabilities
        - storage capacity
    - HPCs often implement real-time OS (RTOS)
    - HPC systems are often rented, leased or shared, which can limit the effectiveness of firewalls and invalidate air gap solutions
    - Securing HPC systems:
        - deploy head nodes and route all outside traffic through them, isolating parts of a system
        - "fingerprint" HPC systems to undersatnd use, and detect anomalous behavior
- **Edge computing**: philosophy of network design where data and compute resources are located as close as possible, at or near the network edge, to optimize bandwidth use while minimizing latency
    - Securing edge computing:
        - this technology creates additional network edges that result in increased levels of complexity
        - visibility, control, and correlation requires a Zero Trust access-based approach to address security on the LAN edge, WAN edge and cloud edge, as well as network management
        - edge-based computing devices,especially IoT devices, are often produced with limited security forethought
        - devices on your network, no matter where they reside, need to be configured, managed, and patched using a consistent policy and enforcement strategy
        - use intelligence from side-channel signals that can pick up hardware trojans and malicious firmware
        - attend to physical security
        - deploy IDS on the network side to monitor for malicious traffic
        - in many scenarios, you are an edge customer, and likely will need to rely on a vendor for some of the security and vulnerability remediation
- **Virtualized systems**: used to host one or more OSs within the memory of a single host computer, or to run apps not compatible with the host OS
    - Securing virtualized systems:
        - the primary component in virtualization is a hypervisor which manages the VMs, virtual data storage, virtual network components
        - the hypervisor represents an additional attack surface
        - in virtualized environments, you need to protect both the VMs and the physical infrastructure/hypervisor
        - hypervisor admin accounts/credentials and service accounts are targets because they often provide access to VMs and their data; these accounts should be protected
        - virtual hosts should be hardened; to protect the host, avoid using it for anything other than hosting virtualized elements

        - virtualized systems should be security tested via vulnerability assessment and penetration testing
        - virtualization doesn't lessen the security management requirements of an OS, patch management is still required
        - be aware of VM Sprawl and Shadow IT
        - **VM escape**: occurs when software within a guest OS is able to breach the isolation protection provided by the hypervisor
        - VM escape minimizaton:
            - keep highly sensitive systems and data on separate physical machines
            - keep all hypervisor software current with vendor-released patches
            - monitor attack, exposure and abuse indexes for new threats to virtual machines (which might be better protected). Often, virtualization administrators have access to all virtual

3.6 Select and determine cryptographic solutions

- Cryptographic lifecycle (e.g., keys, algorithm selection)
    - Keep **Moore's Law** in mind (processing capabilities of state-of-the-art microprocessors double about every 2 years), and have appropriate governance controls in place to ensure that algorithms, protocols, and key lengths selected are sufficient to preserve the integrity of the cryptosystems for as long as necessary to keep secret information safe
    - Specify the cryptographic algorithms (such as AES, 3DES, and RSA) acceptable for use in an organization.
    - Identify the acceptable key lengths for use with each algorithm based on the sensitivity of the information transmitted
    - Enumerate the secure transaction protocols (such as TLS) that may be used
    - As computing power goes up, the strength of cryptographic algorithms goes down. Keep in mind the effective life of a certificate or certificate template, and of cryptographic systems
    - Beyond brute force, you have other issues to consider, such as the discovery of a bug or an issue with an algorithm or system
    - NIST defines the following terms that are commonly used to describe algorithms and key lengths:
        - approved (a specific algorithm is specified as a NIST recommendation or FIPS recommendation),
        - acceptable (algorithm + key length is safe today),
        - deprecated (algorithm and key length is OK to use, but brings some risk),
        - restricted (use of the algorithm and/or key length is deprecated and should be avoided),
        - legacy (the algorithm and/or key length is outdated and should be avoided when possible), and
        - disallowed (algorithm and/or key length is no longer allowed for the indicated use)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
    - **Symmetric** encryption: uses the same key for encryption and decryption
        - symmetric encryption uses a shared secret key available to all users of the cryptosystem
        - symmetric encryption is faster than asymmetric encryption because smaller keys can be used for the same level of protection
        - downside is that users or systems must find a way to securely share the key and hope the key is used only for the specified communication

        - primarily employed to perform bulk encryption and provides only for the security service of confidentiality -"same" is a synonym for symmetric
        - "different" is a synonym for asymmetric
        - total number of keys required to completely connect n parties using symmetric cryptography is given by this formula:
            - **(n(n - 1)) / 2**
    - **Asymmetric** encryption: uses different keys for encryption and decryption
        - Asymmetric (AKA public key, since one key of a pair is available to anybody) algorithms provide convenient key exchange mechanisms and are scalable to very large numbers of users (addressing the two most significant challenges for users of symmetric cryptosystems) - Asymmetric cryptosystems avoid the challenge of sharing the same secret key between users, by using pairs of public and private keys to allow secure communication without the overhead of complex key distribution
        - Besides the public key, there is a private key that should remain private and protected
        - While asymmetric encryption is slower, it is best suited for sharing between two or more parties
        - Most common asymmetric cryptosystems in use today:
            - Rivest-Shamir-Adleman (RSA)
            - Diffie-Hellman
            - ElGamal
            - Eliptical Curve Cryptography (EEC)

- **Public Key Infrastructure (PKI)**: hierarchy of trust relationships permitting the combination of asymmetric and symmetric cryptography along with hashing and digital certificates (giving us hybrid cryptography)

    - A PKI issues certificates to computing devices and users, enabling them to apply cryptography (for example, to send encrypted email messages, encrypt websites or use IPsec to encrypt data communications)
    - Many vendors provide PKI services; you can run a PKI privately and solely for your own org, you can acquire certificates from a trusted third-party provider, or you can do both (which is common)
    - A PKI is made up of
        - **certification authorities (CAs)**: servers that provide one or more PKI functions, such as providing policies or issuing certificates
        - certificates: issued to other certification authorities or to devices and users
        - policies and procedures: such as how the PKI is secured, and
        - templates: a predefined configuration for specific uses, such as a web server template
    - There are other components and concepts you should know for the exam:
        - A PKI can have multiple tiers:
            - single tier means you have one or more servers that perform all the functions of a PKI.
            - two tiers means you often have an offline root CA (a server that issues certificates to the issuing CAs but remains offline most of the time) in one tier, and issuing CAs (the servers that issue certificates to computing devices and users) in the other tier
            - servers in the second tier are often referred to as intermediate CAs or subordinate CAs.
            - three tier means you can have CAs that are responsible only for issuing policies (and they represent the second tier in a three-tier hierarchy)

                - in such a scenario, the policy CAs should also remain offline and be brought online only as needed
            - Generally, the more tiers, the more security (but proper configuration is critical)
                - the more tiers you have, the more complex and costly the PKI is to build and maintain
            - A PKI should have a certificate policy and a certificate practice statement (CSP)
                - certificate policy: documents how your org handles items like requestor identities, the uses of certificates and storage of private keys
                - CSP: documents the security configuration of your PKI and is usually available to the public
            - Besides issuing certificates, a PKI has other duties:
                - a PKI needs to be able to provide certificate revocation information to clients
                - if an administrator revokes a certificate that has been issued, clients must be able to get that information from your PKI
                - storage of private keys and information about issued certificates (can be stored in a database or a directory)
            - PKI uses LDAP when integrating digital certificates into transmissions

- **Key management practices** include safeguards surrounding the creation, distribution, storage, destruction, recovery, and escrow of secret keys

    - Cryptography can be used as a security mechanism to provide confidentiality, integrity, and availability only if keys are not compromised
    - Three main methods are used to exchange secret keys:
        - offline distribution
        - public key encryption, and
        - the Diffie-Hellman key exchange algorithm
    - Key management can be difficult with symmetric encryption but is much simpler with asymmetric encryption
    - There are several tasks related to key management:
        - Key creation
        - **Key distribution**: the process of sending a key to a user or system; it must be secure and it must be stored in a secure way on the computing device
        - Keys are stored before and after distribution; when distributed to a user, it can't hang out on a user's desktop
        - Keys shouldn't be in cleartext outside the crypography device
        - Key distribution and maintenance should be automated (and hidden from the user)
        - Keys should be backed up!
        - **Key escrow**: process or entity that can recover lost or corrupted cryptographic keys
            - **multiparty key recovery**: when two or more entities are required to reconstruct or recover a key
            - **m of n control**: you designate a group of (n) people as recovery agents, but only need subset (m) of them for key recovery
            - **split custody**: enables two or more people to share access to a key (e.g. for example, two people each hold half the password to the key)

        - Key rotation: rotate keys (retire old keys, implement new) to reduce the risks of a compromised key having access
        - Key states:
            - suspension: temporary hold
            - revocation: permanently revoked
            - expiration
            - destruction
        - See NIST 800-57, Part 1

- Digital signatures and digital certificates

    - **Digital signatures**: provide proof that a message originated from a particular user of a cryptosystem, and ensures that the message was not modified while in transit between two parties

        - Digital signatures rely on a combination of two major concepts — public key cryptography, and hashing functions
        - Digitally signed messages assure the recipient that the message truly came from the claimed sender, enforcing nonrepudiation
        - Digitally signed messages assure the recipient that the message was not altered while in transit; protecting against both malicious modification (third party altering message meaning), and unintentional modification (faults in the communication process)
        - Digital signature process does not provide confidentiality in and of itself (only ensures integrity, authentication, and nonrepudiation)

    - Non-repudiation

        - Here non-repudiation refers to methods ensuring certainty about data origins
        - Most common method of non-repudiation is digital signatures
        - Digital signatures rely on certificates
        - If a digital signature was verified with the public key of the sender, then we know that it was created using the sender's private key
        - Private key should only be known to the sender, so the verification proves to the recipient that the signature came from the sender, providing origin authentication
        - The recipient (or anyone else) can demonstrate that process to a third party providing nonrepudiation
        - Data encryption provides confidentiality

    - Integrity (e.g., hashing)

        - Hash Functions have a very simple purpose — they take a potentially long message and generate a unique output value derived from the content of the message called a **message digest**
            - hash function implements encryption with a specified algorithm, but without a key
            - used to ensure message sent by the originator is the same one received by recipient
            - input can be of any length
            - output has a fixed length
            - the hash function is relatively easy to compute for any input

        - the hash function is one-way, meaning it is extremely difficult to determine the input given the hash function output
        - the hash function should be collision-resistant, meaning it is extremely hard to find two messages that produce the same hash value output
        - hashes are used for storing passwords, with email, and for file download integrity verification
    - Hashing and integrity: if the hash generated by sender, and separately by the receiver match, then we have integrity

3.7 Understand methods of cryptanalytic attacks

- **Brute force**: an attack that attempts every possible valid combination for a key or password
    - They involve using massive amounts of processing power to methodically guess the key used to secure cryptographic communications
- **Ciphertext only**:an attack where you only have the encrypted ciphertext message at your disposal (not the plaintext)
    - If you have enough ciphertext samples, the idea is that you can decrypt the target ciphertext based on the ciphertext samples
    - One technique proves helpful against simple ciphers is frequency analysis (counting the number of times each letter appears in the ciphertext)
- **Known plaintext**:in this attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext (the copy); this knowledge greatly assists the attacker in breaking weaker codes
- **Frequency analysis**:an attack where the characteristics of a language are used to defeat substitution ciphers
    - For example in English, the letter "E" is the most common, so the most common letter in an encrypted cyphertext could be a substitution for "E"
    - Other examples might include letters that appear twice in sequence, as well as the most common words used in a language
- **Chosen ciphertext**: in a chosen ciphertext attack, the attacker has access to one or more ciphertexts and their plaintexts; i.e. the attacker has the ability to decrypt chosen portions of the ciphertext message, and use the decrypted portion to discover the key
    - **Differential cryptanalysis**, a type of chosen plaintext attack, is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions; in the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output advanced methods such as differential cryptanalysis are types of chosen plaintext attacks;
        - as an example, an attacker may try to get the receiver to decrypt modified ciphertext, looking for that modification to cause a predictable change to the plaintext
- **Implementation attack**: attempts to exploit weaknesses in the implementation of a cryptography system

    - Focuses on exploiting the software code, not just errors or flaws but the methodology employed to program the encryption system
    - In this type of attack, attackers look for weaknesses in the implementation, such as a software bug or outdated firmware

- **Side-channel**: these attacks seek to use the way computer systems generate characteristic footprints of activity, such as changes in processor utilization, power consumption, or electromagnetic radiation to monitor system activity and retrieve information that is actively being encrypted

    - Similar to an implementation attack, side-channel attacks look for weaknesses outside of the core cryptography functions themselves
    - A side-channel attack could target a computer's CPU, or attempt to gain key information about the environment during encryption or decryption by looking for electromagnetic emissions or the amount of execution time required during decryption.
    - Side-channel characteristics information are often combined together to try to break down the cryptography
    - Timing attack is an example

- **Fault-Injection**: the attacker attempts to compromise the integrity of a cryptographic device by causing some type of external fault

    - For example, using high-voltage electricity, high or low temperature, or other factors to cause a malfunction that undermines the security of the device

- **Timing**: timing attacks are an example of a side-channel attack where the attacker measures precisely how long cryptographic operations take to complete, gaining information about the cryptographic process that may be used to undermine its security

- **Man-in-the-middle (MITM) (AKA on-path)**: in this attack a malicious individual sits between two communicating parties and intercepts all communications (including the setup of the cryptographic session)

    - Attacker responds to the originator's initialization requests and sets up a secure session with the originator
    - Attacker then establishes a second secure session with the intended recipient using a different key and posing as the originator
    - Attacker can then "sit in the middle" of the communication and read all traffic as it passes between the two parties

- **Pass the hash (PtH)**: a technique where an attacker captures a password hash (as opposed to the password characters) and then simply passes it through for authentication and potentially lateral access to other networked systems

    - The threat actor doesn't need to decrypt the hash to obtain a plain text password
    - PtH attacks exploit the authentication protocol, as the passwords hash remains static for every session until the password is rotated
    - Attackers commonly obtain hashes by scraping a system's active memory and other techniques

- Kerberos exploitation:

    - **Overpass the Hash**: alternative to the PtH attack, used when NTLM is disabled on the network (AKA pass the key)
    - **Pass the Ticket**:in this attack, attackers attempt to harvest tickets held in the lsass.exe process
    - **Silver Ticket**: a silver ticket uses the captured NTLM hash of a service account to create a ticket-granting service (TGS) ticket (the silver ticket grants the attacker all the privileges granted to the service account)
    - **Golden Ticket**: if an attacker obtains the hash of the Kerberos service account (KRBTGT), they can create tickets at will within Active Directory (this provides so much power it is referred to as having a golden ticket)
    - **Kerberos Brute-Force**: attackers use the Python script kerbrute.py on Linux, and Rubeus on Windows systems; tools can guess usernames and passwords
    - **ASREPRoast**: ASREPRoast identifies users that don't have Kerberos preauthentication enabled
    - **Kerberoasting**: kerberoasting collects encrypted ticket-granting service (TGS) tickets

- **Ransomware**: a type of malware that weaponizes cryptography

    - using many of the same techniques as other types of malware, ransomware gens an encryption key, and encrypts critical files
    - this encryption renders the data inaccessible to the authorized user or anyone else other than the malware author - often threatning to publically release sensitive data if ransome is not paid - 2020 study, 56% of orgs suffered a ransomeware attack, 27% of orgs who reported an attack chose to pay, on average ~$1.1m
    - seek legal advice prior to engaging with ransomware authors

3.8 Apply security principles to site and facility design

- **Secure facility plan**: outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security, developed through risk assessment and critical path analysis
    - **critical path analysis (CPA)**: a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting components
    - During CPA, evaluate potential **technology convergence**: the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time, which can result in a single point of failure
    - A secure facility plan is based on a layered defense model
    - Site selection should take into account cost, location, and size (but security should always take precedence), that the building can withstand local extreme weather events, vulnerable entry points, and exterior objects that could conceal break-ins
- Facility Design:
    - the top priority of security should always be the protection of the life and safety of personnel
    - in the US, follow the guidelines and requirements from Occupational Safety and Health Administration (OSHA), and Environmental Protection Agency (EPA)
    - **Crime Prevention Through Environmental Design (CPTED)**: a well-established school of thought on "secure architecture"
        - core principle of CPTED is that the design of the physical environment can be managed/manipulated, and crafted with intention in order to create behavioral effects or changes in people present in those areas that result in reduction of crime as well as a reduction of the fear of crime

        - CPTED stresses three main principles:
            - **natural access control**: the subtle guidance of those entering and leaving a building
                - make the entrance point obvious
                - create internal security zones
                - areas of the same access level should be open, but restricted/closed areas should seem more difficult to access
            - **natural surveillance**: any means to make criminals feel uneasy through increased opportunities to be observed
                - walkways/stairways are open, open areas around entrances
                - areas should be well lit
            - **natural territorial**: reinforcement: attempt to make the area feel like an inclusive, caring community
    - Overall goal is to deter unauthorized people from gaining access to a location (or a secure portion), prevent unauthorized personnel from hiding inside or around the location, and prevent unauthorized from committing crime
    - There are several smaller activities tied to site and facility design, such as upkeep and maintenance: if property is run down, unkempt or appears to be in disrepair, it gives attackers the impression that they can act with impunity on the property

3.9 Design site and facility security controls

- Note that alghough the topics in this section cover mostly interior spaces, physical security is applicable to both interior and exterior of a facility

- **Wiring closets/intermediate distribution facilities (IDF)**: A wiring closet or IDF is typically the smallest room that holds IT hardware

    - Wiring closet is AKA premises wire distribution room, main distribution frame (MDF), intermediate distribution frame (IDF), and telecommunications room, and it is referred to as an IDF in (ISC)^2 CISSP objective 3.9.1
    - Usually includes telephony and network devices, alarm systems, circuit breaker panels, punch-down blocks, WAPs, video/security
    - May include a small number of servers
    - Access to the wiring closest/IDF should be restricted to authorized personnel responsible for managing the IT hardware - Use door access control (i.e. electronic badge system or electronic combination lock)
    - From a layout perspective, wiring closets should be accessible only in private areas of the building interiors; people must pass through a visitor center and a controlled doorway prior to be able to enter a wiring closet

- **Server rooms/data centers**: server rooms, data centers, communication rooms, server vaults, and IT closets are enclosed, restricted, and protected rooms where mission critical servers and networks are housed

    - A server room is a bigger version of a wiring closet, much smaller than a data center
    - A server room typically houses network equipment, backup infrastructure and servers (more archaic versions include telephony equipment)

    - Server rooms should be designed to support optimal operation of IT infrastructure and to block unauthorirzed human access or intervention
    - Server rooms should be located at the core of the building (avoid ground floor, top floor, or in the basement)
    - Server rooms should have a single entrance (and an emergency exit)
    - Server room should block unauthorized access, and entries and exits should be logged
    - Datacenters are usually more protected than server rooms, and can include guards and mantraps
    - Datacenters can be single-tenant or multitenant

- **Media storage facilities**:often store backup tapes and other media, and should be protected just like a server room

    - Depending on requirements a cabinet or safe could suffice
    - New blank media, and media that is reused (e.g. thumb drives, flash memory cards, portable hard drives) should be protected against theft and data remnant recovery
    - Other recommendations:
        - employ a media librarian or custodian
        - use check-in/check-out process for media tracking
        - run a secure drive sanitization or zeroization when media is returned
    - Note: a safe is a movable secured container that's not integrated into a building's construction; a vault is a permanent safe integrated into construction

- **Evidence storage**: as cybercrime events continue to increase, it is import to retain logs, audit trails, and other records of digital events; the evidence storage exists to preserve chain of custody

    - A key part of incident response is to gather evidence to perform root cause analysis
    - An evidence storage room should be protected like a server room or media storage facility
    - An evidence storage room can contain physical evidence (such as a smartphone) or digital evidence (such as a database)

- **Restricted and work area security**: covers the design and configuration of internal security, including work and visitor areas

    - Includes areas that contain assets of higher value/importance which should have more restricted access
    - Restricted work areas are used for sensitive operations, such as network/security ops
    - Protection should be similar to a server room, but video surveillance is typically limited to entry and exit points

- Utilities and heating, ventilation, and air conditioning (HVAC)

    - Power management in ascending order: surge protectors, power/power-line conditioner, uninterruptible power supply (UPS), generators
    - Types of UPS:
        - double conversion: functions by taking power from the wall outlet, storing it in a battery, pulling power out of the battery and feeding that power to the device/devices
        - line-interactive: has a surge protector, battery charger/inverter and voltage regulator positioned between the grid power source and the equipment (battery is not in line under normal conditions)

    - Commercial power problem types:
        - **fault**: momentary loss of power
        - **blackout**: complete loss of power
        - **sag**: momentary low voltage
        - **brownout**: prolonged low voltage
        - **spike**: momentary high voltage
        - **surge**: prolonged high voltage
        - **inrush**: initial surge of power associated with connecting to a power source
    - Think through types of physical controls for HVAC:
        - restrict duct space continuity to controlled areas
        - use separate and redundant HVAC systems for computer equipment
    - Datacenter:
        - should be on different power circuits from occupied areas
        - common to use a backup generator

- Environmental issues

    - Environmental monitoring is the process of measuring and evaluating the quality of the environment within a given structure (e.g. temperature, humidity, dust, smoke), using things like chemical, biological, radiological, and microbiological detectors
    - Halon starves a fire of oxygen by disrupting the chemical reaction of combustion, but degrades into toxic gases at 900 degrees Fahrenheit, and is not environmentally friendly
    - If water-based sprinklers are used for fire suppression, damage to electronic equipment is likely; automate the shutoff of electricity prior to sprinkler trigger
    - Other environmental issues include earthquakes, power outages, tornados and wind
    - Secondary facilities should be located far enough away from the primary to ensure they won't be damaged by the same event

- Fire prevention, detection and suppression

    - Protecting personnel from harm should always be the most important goal of any security or protection system!
    - In addition to protecting people, fire detection and suppression is designed to keep asset damage caused by fire, smoke, heat, and suppression materials to a minimum
    - **Fire triangle**: three represent fuel, heat, and oxygen; the center of the triangle represents the chemical reaction among these three elements
        - if you can remove any one of the four items from the fire triangle, the fire can be extinguished
    - Fire suppression mediums:
        - water suppresses temperature
        - soda acid and other dry powders suppress the fuel supply
        - carbon dioxide (CO_2) suppresses the oxygen supply
        - halon substitutes and other nonflammable gases interfere with the chemistry of combustion and/or suppress the oxygen supply
    - Fire stages:
        - **Stage 1**: incipient stage: at this stage, there is only air ionization and no smoke

        - **Stage 2**: smoke stage: smoke is visible from the point of ignition
        - **Stage 3**: flame stage: this is when a flame can be seen with the naked eye
        - **Stage 4**: heat stage: at stage 4, there is an intense heat buildup and everything in the area burns
    - Fire extinguisher classes:
        - **Class A**: common combustibles
        - **Class B**: liquids
        - **Class C**: electrical
        - **Class D**: metal
        - **Class K**: cooking material (oil/grease)
    - Four main types of suppression:
        - **wet pipe system**: (AKA closed head system): is always filled with water. water discharges immediately when suppression is triggered
        - **dry pipe system**: contains compressed inert gas
        - **preaction system**: a variation of the dry pipe system that uses a two-stage detection and release mechanism
        - **deluge system**: uses larger pipes and delivers larger volume of water
    - Note: Most sprinkler heads feature a glass bulb filled with a glycerin-based liquid; this liquid expands when it comes in contact with air heated to between 135 and 165 degrees; when the liquid expands, it shatters its glass confines and the sprinkler head activates

- Power (e.g., redundant, backup)

    - Consider designing power to provide for high availability
    - Most power systems have to be tested at regular intervals
    - As part of the design, mandate redundant power systems to accommodate testing, upgrades and other maintenance
    - Additionally, test failover to a redundant power system and ensure it is fully functional
    - The International Electrical Testing Association (NETA) has developed standards around testing power systems
    - Battery backup/fail-over power (including UPS/generators):
        - this is a system that collects power into a battery but can switch over to pulling power from the battery when the power grid fails
        - generally, this type of system was implemented to supply power to an entire building rather than just one or a few devices

Domain 4 **Communication and Network Security**

Networking can be one of the more complex exam topics; if you have a networking background, you likely won't find this domain difficult-- if not, spend extra time in this section and consider diving deeper into topics that are fuzzy

4.1 Assess and implement secure design principles in network architectures

- **OSI**: Open Systems Interconnection (OSI) Reference Model developed by ISO (International Organization for Standardization) to establish a common communication structure or standard for all computer systems; it is an abstract framework

- Communication between layers via **encapsulation** (at each layer, the previous layer's header and payload become the payload of the current layer) and **deencapsulation** (inverse action occurring as data moves up layers)

Layer	OSI model layer	TCP/IP model	PDU	Devices	Protocols
7	Application	Application	Data	L7 firewall	HTTP/s, DNS, DHCP, FTP,S-HTTP, TPFT, Telnet, SSH, SMTP, POP3, PEM, IMAP, NTP, SNMP, TLS/SSL, GBP, RIP, SIP, S/MIME etc.
6	Presentation	Application	Data	L7 firewall	All the above
5	Session	Application	Data	L7 firewall	All the above
4	Transport	Transport (host-to-host)	Segments	L4 firewall	TCP (connection oriented), UDP (connectionless)
3	Network	Internet/IP	Packets	Router, Multiplayer Switch, Router	IPv4, IPv6, IPSec, OSPF, EIGRP
2	Data Link	Network Access	Frames	Switch, Bridge, NIC, Wireless Access Point	MAC, ARP Ethernet 802.3 (Wired), CDP, LLDP, HDLC, PPP, DSL, L2TP, IEEE 802.11 (Wireless), SONET/SDH
1	Physical	Network Access	Bits	All the above	Electrical signal (copper wire), Light signal (optical fibre), Radio signal (air)

OSI layers in details

- Mnemonics:
  - from top: All People Seem To Need Delicious Pizza
  - from bottom: Please Do Not Throw Sausage Pizza Away
- Application Layer (7)
  - Responsible for:
    - interfacing user applications, network services, or the operating system with the protocol stack
    - identifying and establishing availability of communication partners
    - determining resource availability and
    - synchronizing communication
- Presentation Layer (6)
  - Responsible for transforming data into the format that any system following the OSI model can understand
  - Associated tasks:
    - data representation

        - character conversion
        - data compression
        - data encryption

- Session Layer (5)

    - Responsible for establishing, maintaining, and terminating communication sessions between two computers
    - Three communication session phases:
        - connection establishment
            - **simplex**: one-way
            - **half-duplex**: both comm devices can transmit/receive, but not at the same time
            - **full-duplex**: both comm devices can transmit/receive at same time
        - data transfer
        - connection release

- Transport Layer (4)

    - Responsible for managing the integrity of a connection and controlling the session; providing transparent data transport and end-to-end transmission control
    - Defines session rules like how much data each segment can contain, how to verify message integrity, and how to determine whether data has been lost
    - Protocols that operate at the Transport layer:
        - Transmission Control Protocol (TCP)
            - full-duplex, connection-oriented protocol
            - uses three-way handshake
        - User Datagram Protocol (UDP)
            - connectionless protocol that provides fast, best-effort delivery of **datagrams** (self-container unit of data)
        - Transport Layer Security (TLS)

- Network Layer (3)

    - Responsible for logical addressing, and providing routing or delivery guidance (but not necessarily verifying guaranteed delivery), manages error detection and traffic control
    - **routing protocols**: move routed protocol messages across a network
        - includes RIP, OSPF, IS-IS, IGRP, and BGP
        - routing protocols are defined at the Network Layer and specify how routers communicate
        - routing protocols can be static or dynamic, and categorized as interior or exterior
        - **static routing protocol**: requires an admin to create/update routes on the router
        - **dynamic**: can discover routers and determine best route to a given destination; routing table is periodically updated
        - **distance-vector**: (interior) makes routing decisions based on distance (e.g. hop count), and vector (router egress interface); examples:
            - **Routing Information Protocol (RIP)**: a distance-vector protocol that uses hop count as its routing metric

        - Interior Gateway Routing Protocol (IGRP)
        - Enhanced Interior Gateway Routing Protocol (EIGRP)
    - **link state**: (interior) uses router characteristics (e.g. speed, latency, error rates) to make next hop routing decisions; examples:
        - Open Shortest Path First (OSPF)
        - Intermediate System to Intermediate System (IS-IS)
    - interior vs exterior:
        - interior routing protocols ("myopic") make next hop decisions based only on info related to the next immediate hop
        - exterior routing protocols ("far-sighted") make hop decisions based on the entire remaining path (i.e.) vector
        - **Border Gateway Protocol (BGP)**: an exterior/path vector protocol
  - Routed protocols include Internetwork Package Exchange (IPX) and Internet Protocol (IP)
  - IP is part of the TCP/IP (Transmission Control Protocol/Internet Protocol) suite
    - IP provides the foundation for other protocols to be able to communicate; IP itself is a connectionless protocol
    - IPv4 uses 32-bit addresses
    - IPv6 uses 128-bit addresses
    - TCP or UDP is used to communicate over IP
    - IPSec provides data authentication, integrity and confidentiality
  - **logical address**: occurs when an address is assigned and used by software or a protocol rather than being provided/controlled by hardware
  - Network layer's packet header includes the source and destination IP addresses

- Data Link Layer (2)

  - Responsible for formatting a packet for transmission
  - Adds the source and destination hardware addresses to the frame
  - Media Access Control (MAC) - (hardware-based) address/AKA NIC address
    - MAC address is a 6-byte (48-bit) binary address written in hex
        - first 6b/48-bits: Organizationally Unique Identifier (OUI) - denotes manufacturer
        - last 3b/24-bits: unique to that interface
  - **Address Resolution Protocol (ARP)**: operates at layer 2
  - Switches & bridges function at this layer

- Physical Layer (1)

  - Converts a frame into bits for transmission/receiving over the physical connection medium
  - Network hardware devices that function at layer 1 include NICs, hubs, repeaters, concentrators, amplifiers
  - Know four basic network topologies:
    - **star**: each individual node on the network is directly connect to a switch/hub/concentrator
    - **mesh**: all systems are interconnected; partial mesh can be created by adding multiple NICs or server clustering
    - **ring**: closed loop that connects end devices in a continuous ring (all communication travels in a single direction around the ring);

        - **Multistation Access Unit** (MSAU or MAU) connects individual devices
        - used in token ring and FDDI networks
      - **bus**: all devices are connected to a single cable (backbone) terminated on both ends
    - Know commonly used twisted-pair cable categories
    - Know cable types & characteristics

TCP/IP layers

- Network Access Layer: defines the protocols and hardware required to deliver data across a physical network
- Internet Layer: defines the protocols for logically transmitting packets over the network
- Transport Layer: defines protocols for setting up the level of transmission service for applications; this layer is responsible for the reliable transmission of data and the error-free delivery of packets
- Application Layer: defines protocols for node-to-node application communication and provides services to the application software running on a computer

Secure protocols

- **Kerberos**: standards-based network authentication protocol, used in many products (most notably Microsoft Active Directory Domain Services or AD DS)
    - Kerberos is mostly used on LANs for organization-wide authentication, single sign-on (SSO) and authorization
- SSL and TLS: data protection used for protecting website transactions (e.g. banking, ecommerce)
    - SSL and TLS both offer data encryption, integrity and authentication
    - TLS has suplanted SSL (the original protocol, considered legacy/insecure)
    - TLS was initially introduced in 1999 but didn't gain widespread use until years later
    - The original versions of TLS (1.0 and 1.1) are considered deprecated and organizations should be relying on TLS 1.2 or TLS 1.3
- **SFTP**: a version of FTP that includes encryption and is used for transferring files between two devices (often a client / server)
- **SSH**: remote management protocol, which operates over TCP/IP
    - all communications are encrypted
    - primarily used by IT administrators to manage devices such as servers and network devices
- **IPSec**: an IETF standard suite of protocols that is used to connect nodes (e.g. computers or office locations) together
    - widely used in virtual private networks (VPNs)
    - IPSec provides encryption, authentication and data integrity

Micro-Segmentation

- **Software-defined networks (SDN)**:
    - SDN is effectively network virtualization, and separates the infrastructure layer (aka the data or forwarding plane) - hardware and hardware-based settings, from the control layer - network services of data transmission management
        - NOTE: the **control plane**: uses protocols to decide where to send traffic, and the **data plane**: includes rules that decide whether traffic will be forwarded
    - typically ABAC-based
    - an SDN solution provides the option to handle traffic routing using simpler network devices that accept instructions from the SDN controller
    - SDN offers a network design that is directly programmable from a central location, is flexible, vendor neutral, and based on open standards
    - Allows org to mix/match hardware
- **Virtual extensible local area network (VXLAN)**:
    - an encapsulation protocol that enables VLANs to be stretched across subnets and geographic distances
    - Typically restricted to layer 2
    - Allows up to 16 million virtual networks (VLAN limit is 4096)
    - VXLAN can be used as a means to implement microsegmentation without limiting segments to local entities only
    - Defined in RFC 7348
- Encapsulation:
    - the OSI model represents a protocol stack, or a layered collection of multiple protocols, and communication between protocol layers occurs via encapsulation and deencapsulation (defined above)
- **Software-defined wide area network (SD-WAN)**: an evolution of SDN that can be used to manage the connectivity and control services between distant data centers, remote locations, and cloud services over WAN links

Wireless Networks

- Li-Fi: **light fidelity (Li-Fi)**: a form of wireless communication technology that relies on light to transmit data, with theorectical speeds up to 224Gbits/sec
- Wi-Fi:
    - **Wired Equivalent Privacy (WEP)**:
        - WEP is defined by the original IEEE 802.11 standard
        - WEP uses a predefined shared Rivest Cipher 4 (RC4) secret key for both authentication (SKA) and encryption
        - Shared key is static
        - WEP is weak from RC4 flaws
    - Wi-Fi Protected Access II (WPA2):
        - IEEE 802.11i WPA2 replaced WEP and WPA

        - Uses AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
    - Frequency table:

Amendment	Wi-Fi Alliance	Speed	Frequency
802.11	--	2 Mbps	2.4 GHz
802.11a	Wi-Fi 2	54 Mbps	2.4 GHz
802.11b	Wi-Fi 1	11 Mbps	2.4 GHz
802.11g	Wi-Fi 3	54 Mbps	2.4 GHz
802.11n	Wi-Fi 4	200+ Mbps	2.4 GHz
802.11ac	Wi-Fi 5	1 Gbps	2.4 GHz
802.11ax	Wi-Fi 6/Wi-Fi 6E	9.5 Gbps	2.4 GHz

- **Zigbee**: IoT equipment communications concept based on Bluetooth
    - Low power/low throughput
    - Requires close proximity
    - Encrypted using 128-bit symmetric algorithm
- **Satellite**: primarily uses radio waves between terrestrial locations and an orbiting artificial satellite
    - Supports telephone, tv, radio, internet, military communications
    - 3 primary orbits:
        - LEO: low Earth orbit (160-2k km)
            - have stronger signals
            - multiple devices needed to maintain coverage (e.g. Starlink)
        - MEO: medium Earth orbit (2k-35768 km)
            - above a terrestrial location longer than LEO
            - higher orbit, additional delay/weaker signal
        - GEO: geostationary orbit (35768 km)
            - maintain a fixed position above a terrestrial location, and ground stations can use fixed antennas
            - larger transmission footprint than MEO, but higher latency

Cellular Networks

- A cellular network or a wireless network is the primary communications technology used by many mobile devices
- Cells are primary transceiver (cell site/tower)
- Generally encrypted between mobile device and transmission tower; plaintext over wire; use encryption like TLS/VPN
- 4G
    - 4G allows for mobile devices to achieve 100 Mbps, and stationary devices can reach 1 Gbps
    - LTE and WiMAX are common transmission systems
- 5G
    - 5G uses higher frequencies than previous tech, allowing for higher transmission speeds — up to 10 Gbps, but at reduced distances
    - Orgs need to enforce security requirements on 5G
- Security issues with wireless:

- provider network (voice or data) is not necessarily secure
- your cell phone can be intercepted
- provider's towers can be simulated to conduct man-in-the-middle/on-path attack
- using cell connectivity to access the internet or your office network creates a potential bridge, provider attackers with another avenue

Content Distribution Network (CDN): a collection of resource services deployed in numerous data centers across the internet in order to provide low latency, high performance, and high availability of the hosted content

- CDNs provide multimedia performance quality through the concept of distributed data hosts, geographically distributed, closer to groups of customers
- Provides geographic and logical load balancing; lower-latency and higher-quality throughput
- Client-based CDN is often referred to as P2P (peer-to-peer)

4.2 Secure network components

The components of a network make up the backbone of the logical infrastructure for an organization. These components are often critical to day-to-day operations, and an outage or security issue can be very costly

Here are issues to pay attention to:

- Operation of hardware (e.g. redundant power, warranty, support)
    - Modems are a type of Channel Service Unit/Data Service Unit (CSU/DSU) typically used for converting analog signals into digital; the CSU handles communication to the provider network, the DSU handles communication with the internal digital equipment (in most cases, a router)
        - Modems typically operate at Layer 2
        - Routers operate at Layer 3, and make the connection from a modem available to multiple devices in a network, including switches, access points and endpoint devices
        - Switches are typically connected to a router to enable multiple devices to use the connection
        - Switches help provide internal connectivity, as well as create separate broadcast domains when configured with VLANs
        - Switches typically operate at Layer 2 of the OSI model, but many switches can operate at both Layer 2 and Layer 3
        - Access points can be configured in the network topology to provide wireless access using one of the protocols and encryption algorithms
    - Redundant power: most home equipment use a single power supply, if that supply fails, the device loses power
        - redundant power is typically used with components such as servers, routers, and firewalls
        - redundant power is usually paired with other types of redundancies to provide high availability
- Transmission Media: come in many forms, not just cables
    - Includes wireless, LiFi, Bluetooth, Zigbee, satellites
    - Most common cause of network failure (i.e. violations of availability) are cable failures or misconfigurations
    - Wired transmission media can typically be described in three categories: coaxial, Ethernet, fiber

- Coaxial is typically used with cable modem installations to provide connectivity to an ISP, and requires a modem to convert the analog signals to digital
    - fairly resistent to EMI
    - longer lengths than twisted pair
    - requires segment terminators
    - two main types:
        - **thinnet (10Base2)**: used to connect systems to backbond trunks of thicknet cabling (185m, 10Mbps)
        - **thicknet (10Base5)**: can span 500 meters and provide up to 10Mbps
- Ethernet can be used to describe many mediums, it is typically associated with Category 5/6 unshielded twisted-pair (UTP) or shielded twisted pair (STP), and can be plenum-rated
- Fiber typically comes in two options: single-mode or multi-mode
    - Single-mode is typically used for long-distance communication, over several kilometers or miles
    - Multi-mode fiber is typically used for faster transmission, but with a distance limit depending on the desired speed
    - Fiber is most often used in the datacenter for backend components

Category	Throughput Notes
Cat 1	1 Mbps
Cat 2	4 Mbps
Cat 3	10 Mbps
Cat 4	16 Mbps
Cat 5	100 Mbps
Cat 5e	1 Gbps
Cat 6	1 Gbps
Cat 6a	10 Gbps
Cat 7	10 Gbps
Cat 8	40 Gbps

- Network Access Control (NAC) devices
    - NAC is the concept of controlling access to an environment through strict adherence to and enforcement of security policy
    - NAC is meant to be an automated detection and response system that can react in real time to ensure that all monitored systems are patched/updated and have current security configurations, as well as keep unauthorized devices out of the network
    - NAC goals:
        - prevent/reduce known attacks directly and zero-day indirectly
        - enforce security policy throughout the network
        - use identities to perform access control
    - NAC can be implemented with a preadmission or postadmission philosophy:
        - **preadmission philosohpy**: requires a system to meet all current security requirements (such as patch application and malware scanner updates) before it is allowed to communicate with the network

        - **postadmission philosophy**: allows and denies access based on user activity, which is based on a predefined authorization matrix
    - Agent-based NAC:
        - Installed on each management system, checks config files regularly, and can quarantine for non-compliance
        - Dissolvable:usually written in a web/mobile language and is executed on each local machine when the specific management web page is accessed (such as captive portal);
        - Permanent: installed on the monitored system as a persistent background service
    - Just as you need to control physical access to equipment and wiring, you need to use logical controls to protect a network; there are a variety of devices that provide this type of protection, including:
        - Stateful and stateless firewalls can perform inspection of the network packets and use rules, signatures and patterns to determine whether the packet should be delivered
            - reasons for dropping a packet could include addresses that don't exist on the network, ports or addresses that are blocked, or the content of the packet (e.g malicious packets blocked by administrative policy)
        - Intrusion detection and prevention devices which monitor the network for unusual network traffic and MAC or IP address spoofing, and then either alert on or actively stop this type of traffic
        - Proxy/reverse proxies:
            - proxy servers can be used to proxy internet-bound traffic,instead of letting clients talk directly
            - reverse proxies are often deployed to a perimeter network; they proxy communication from the internet to an internal host, such as a web server
            - like a firewall, a reverse proxy can use rules and policies to block certain types of communication

- Endpoint security: each individual device must maintain local security

    - Any weakness in a network, whether border, server, or client-based presents a risk to all elements of the organization
    - Client/Server model is a distributed architecture, which means that security must be addressed everywhere instead of at a single centralized host
    - Processing, storage on clients and servers, network links, communication equipment all must be secured
    - Clients must be subjected to policies that impose safeguards on their content and users' activities including:
        - email
        - upload/download policies and screening
        - subject to robust access controls (e.g. MFA)
        - file encryption
        - screen savers
        - isolated processes for user/supervisor modes
        - local files should be backed up
        - protection domains/network segments
        - security awareness training
        - desktop env should be included in org DR

        - EDR/MDR should be considered

4.3 Implement secure communication channels according to design

- Protocols that provide security services for application-specific communication channels are called secure communication protocols

- Voice

    - as more organizations switch to VoIP, protocols like SIP become more common, and introducing additional management, either via dedicated voice VLANs, or by establishing quality of service (QoS) levels to ensure voice traffic priority
    - web-based voice apps can be more difficult to manage, causing additional unplanned bandwidth consumption

- Multimedia collaboration

    - there are a variety of new technologies that allow instant organizational collaboration, including smartboards, and products that enhance on-site, hybrid, or virutal meetings
    - mobile communication apps are a huge market, and will continue to grow, increasing the complexity of mobile security

- Remote access

    - 4 main types of remote access:
        - **service specific**: gives users the ability to remotely connect to and manipulate or interact with a single service (e.g. email)
        - **remote-control**: grants a remote user the ability to fully control another system that is physically distant
        - **remote node operation**: AKA remote client connecting directly to a LAN
        - **screen scraping**: refers to 1) remote control, remote access, or remote desktop services or 2) technology that allows an automated tool to interact with a human interface
    - VPN: virtual private network is a traditional remote access technology
    - WAP (local env treats as remote access)
    - VDI(virtual desktop infrastructure) / VMI (virtual mobile interface)
    - jumpbox: a jump server/jumpbox is a remote access system deployed to make accessing a specific system or network easier or more secure
        - often deployed in extranets, screened subnets, or cloud networks where a standard direct link or private channel is not available
    - RDS (Remote Desktop Service) such as RD, Teamviewer, VNC etc can provide in-office experience while remote
    - using cloud-based desktop solutions such as Amazon Workspaces, Amazon AppStream, V2 Cloud, and Microsoft Azure
    - security must be considered to provide protection for your private network against remote access complications:
        - stringent auth before granting access
        - grant permission only for specific need

        - remote comm protected via encryption
    - create a remote access security policy, addressing:
        - remote connectivity technology
        - transmission protectio
        - authentication protection
        - remote user assistance

- Data communications

    - whether workers are physically in an office or working remotely, communication between devices should be encrypted to prevent any unauthorized device or person from openly reading the contents of packets as they are sent across a network
    - corporate networks can be segmented into multiple VLANs to separate different types of resources
    - communications should be encrypted using TLS or IPSec

- Virtualized networks

    - allow adopting of things like software-defined networks, VLANs, virtual switches, virtual SANs, guest operating systems, port isolation etc
    - many organizations are moving to the cloud, and not continuing to build out local or on-site server infrastructure
    - however, organizations still use hypervisors to virtualize servers and desktops for increased density and reliability
        - to host multiple servers on a single hypervisor, the Ethernet and storage networks must also be virtualized
        - VMware vSphere and Microsoft Hyper-V both use virtual network and storage switches to allow communication between virtual machines and the physical network; guest operating systems running in the VMs use a synthetic network or storage adapter, which is relayed to the physical adapter on the host
        - software-defined networking on the hypervisor can control the VLANs, port isolation, bandwidth and other aspects just as if it was a physical port

- Third-party connectivity

    - any time an org's network is connected directly to another entity's network, their local threats and risks affect each other
        - **memorandum of understanding (MOU)** (MOU = letter of intent) or **memorandum of agreement (MOA)**: an expression of agreement or aligned intent, will, or purpose between two entities
        - **interconnection security agreement (ISA)**: a formal declaration of the security stance, risk, and technical requirements of a link between two organizations' IT infrastructures
    - remote workers are another form of third-party connectivity
    - vendors (like IT auditing firms) may need to connect to your network, and attackers are routinely looking for creative ways to gain organizational access -- third-party connectivity is one option
    - as organizations evaluate third-party connectivity, they need to look carefully at the principle of least privilege and at methods of monitoring use and misuse

Domain 5 **Identity and Access Management (IAM)**

The identity and Access Management (IAM) domain focuses on issues related to granting and revoking privileges to access data or perform actions on systems

- Assets include information, systems, devices, facilities, and applications
- Organizations use both physical and logical access controls to protect them
- Identification is the process of a subject claiming, or professing, an identity
- Authentication verifies the subject's identity by comparing one or more authentication factors against a database holding authentication info for users
- The three primary authentication factors are something you know, something you have, and something you are
- Single sign-on (SSO) technologies allow users to authenticate once and access any resources in a network or the cloud, without authenticating again
- Federated Identity Management (FIM) systems link user identities in one system with other systems to implement SSO

5.1 Control physical and logical access to assets (OSG-9 Chpt 13)

- Controlling access to assets (tangible: things you can touch, or nontangible: info and data) is a central theme of security
- In addition to personnel, assets can be information, systems, devices, facilities, or applications:
    - 5.1.1 Information: an org's information includes all of its data, stored in simple files (on servers, computers, and small devices), or in databases
    - 5.1.2 Systems: an org's systems include anything that provide one or more services; a web server with a database is a system; permissions assigned to user and system accounts control system access
    - 5.1.3 Devices: refers to any computing system (e.g. routers & switches, smartphones, laptops, and printers); BYOD has been increasingly adopted, and the data stored on the devices is still an asset to the org
    - 5.1.4 Facilities: any physical location, building, rooms, complexes etc; physical security controls are important to help protect facilities
    - 5.1.5 Applications: apps provide access to data; permissions are an easy way to restrict logical access to apps
- Understand what assets you have, and how to protect them
    - **physical security controls**: such as perimeter security and environmental controls
        - control access and the environment
    - **logical access controls**: technical controls used to protect access to information, systems, devices, and applications
        - includes authentication, authorization, and permissions
        - permissions help ensure only authorized entities can access data
        - logical controls restrict access to config settings on systems/networks to only authed individuals
        - applies to on-prem and cloud

5.2 Manage identification and authentication of people, devices, and services (OSG-9 Chpt 13)

- **Identification**: the process of a subject claiming, or professing an identity

- **Authentication**: verifies the subject's identity by comparing one or more factors against a database of valid identities, such as user accounts
    - a core principle with authentication is that all subjects must have unique identities
    - identification and authentication occur together as a single two-step process
    - users identify themselves with usernames and authenticate (or prove their identity) with passwords
- 5.2.1 Identiy management (IdM) implementation
    - Identity and access management is a collection of processes and techologies that are used to control access to critical assets; it's purpose is the management of access to information, systems, devices, and facilities
    - Identity Management (IdM) implementation techniques generally fall into two categories:
        - **centralized access control**: implies a single entity within a system performs all authorization verification
            - potentially creates a single point of failure
            - small team can manage initially, and can scale to more users
        - **decentralized access control**: (AKA distributed access control) implies several entities located throughout a system perform auth verification
            - requires more individuals or teams to manage, and admin may be spred across numerous locations
            - difficult to maintain consistency
            - changes made to any individual access control point needs to be repeated at others
    - With ubiquitious mobile computing and anywhere, anytime access (to apps & data), identity is the "new perimeter"
- 5.2.2 Single/Multi-Factor Authentication (MFA)
    - **Single-factor authentication**: any authentication using only one proof of identity
    - **Two-factor authentication (2FA)**: requires two different proofs of identity
    - **Multifactor authentication (MFA)**: any authentication using two or more factors
        - multifactor auth must use multiple types or factors, such as something you know and something you have
        - note: requiring users to enter a password and a PIN is NOT multifactor (both are something you know)
    - Two-factor methods:
        - **Hash Message Authentication Code (HMAC)**: includes a hash function used by the HMAC-based One-Time Password (HOTP) standard to create onetime passwords
        - **Time-based One-Time Password (TOTP)**: similar to HOTP, but uses a timestamp and remains valid for a certain time frame (e.g. 30 or 60 seconds)
            - e.g. phone-based authenticator app, where your phone is mimicking a hardware TOTP token (combined with userid/password is considered two-factor or two-step authentication)
        - **Email challenge**: popular method, used by websites, sending the user an email with a PIN
        - Short Message Service (SMS) to send users a text with a PIN is another 2-factor method; note that NIST SP 800-63B points out vulnerabilities, and deprecates use of SMS as a two-factor method for federal agencies
- 5.2.3 Accountability
    - Two important security elements in an access control system are authorization and accountability
        - **Authorization**: subjects are granted access to objects based on proven identities

        - **Accountability**: users and other subjects can be held accountable for their actions when auditing is implemented
    - **Auditing**: tracks subjects and records when they access objects, creating an audit trail in one or more audit logs
    - Auditing provides accountability
- 5.2.4 Session management
    - Session management is important to use with any type of authentication system to prevent unauthorized access
    - Desktop/laptops: recommendation to use screensavers, although modern OSs have timeout/lock features
    - Secure online sessions should terminate after a timeout period
    - The Open Web Application Security Project (OWASP) publishes “cheat sheets” that provide app developer’s specific recommendations
- 5.2.5 Registration, proofing, and establishment of identity
    - Within an organization, new employees prove their identity with appropriate documentation during the hiring process
        - in-person identity proofing includes things like passport, DL, birth cert etc
    - Online orgs often use knowledge-based authentication (KBA) for identity-proofing of someone new (e.g. a new customer creating a new bank/savings account)
        - example questions include past vehicle purchases, amount of mortgage payment, previous addresses, DL numbers
        - they then query authoritative information (e.g. credit bureaus or gov agencies) for matches
    - Cognitive Passwords: security questions that are gathered during account creation, which are later used as questions for authentication (e.g. name of pet, color of first car etc)
        - one of the flaws associated with cognitive passwords is that the information is often available on social media sites or general internet searches
- 5.2.6 Federated Identity Management (FIM)
    - Federated Identity Management (FIM) systems (a form of SSO) are often used by cloud-based apps
    - A federated identity links a user’s identity in one system with multiple identity management systems
    - FIM allows multiple orgs to join a federation or group, agreeing to share identity information
        - users in each org can log in once in their own org, and their credentials are matched with a federated identity
        - users can then use this federated identity to access resources in any other org within the group
        - where each organization decides what resources to share
    - Methods used to implement federated identity management systems include:
        - Security Assertion Markup Language (SAML)
        - OAuth
        - OpenID Connect (OIDC)
    - Cloud-based federation typically uses a third-party service to share federated identities
    - Federated identity management systems can be hosted on-premises, in the cloud, or in a combination of the two as a hybrid system
- 5.2.7 Credential management systems
    - **Credential management systems**: provide storage space for usernames and password
        - e.g. web browsers that remember usernames and passwords for visited sites

    - The World Wide Web Consortium (W3C) published the Credential Management Level 1 API as a working draft in January 2019, which many browsers have adopted
    - Some federated identity management solutions use the Credential Management API, allowing web apps to implement SSO using a federated identity provider
        - e.g. using your Google or Facebook account to sign into Zoom
- 5.2.8 Singe Sign On (SSO)
    - **Single Sign-On (SSO)**: a centralized access control technique allowing a subject to be authenticated once on a system and access multiple resources without authenticating again
    - Advantages of using SSO include:
        - reduces the number of passwords that users need to remember, and they are less likely to write them down
        - eases administration by reducing the number of accounts
    - Disadvantages:
        - once an account is compromised, an attacker gains unrestricted access to all of the authorized resources
    - Within an organization, a central access control system, such as a directory service, is often used for SSO
        - **directory service**: a centralized database that includes information about subjects and objects, including authentication data
        - many directory services are based on the Lightweight Directory Access Protocol (LDAP)
- 5.2.9 Just-In_time (JIT)
    - Federated identity solutions that support just-in-time (JIT) provisioning automatically create the relationship between two entities so that new users can access resources
    - A JIT solution creates the connection without any administrative intervention
    - JIT systems commonly use SAML to exchange required data

5.3 Federated Identity with a third-party service (OSG-9 Chpt 13)

- 5.3.1 On-premise
    - Federated identity management can be hosted on-premise, and typically provides an organization with the most control
- 5.3.2 Cloud
    - Cloud-based apps used federated identify management (FIM) systems, which are a form of SSO
    - Cloud-based federation typically uses a third-party service to hsare federated identities (e.g. training sites use federated SSO systems)
        - commonly matching the user's internal login ID with a federated identify
- 5.3.3 Hybrid
    - A hybrid federation is a combination of a cloud-based solution and an on-premise solution

5.4 Implement and manage authorization mechanisms (OSG-9 Chpt 14)

- 5.4.1 Role Based Access Control (RBAC)
    - A key characteristic of the Role-Based Access Control (RBAC) model is the use of roles or groups
    - Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles (typically defined by job function)
        - if the user account is in a role, the user has all privileges assigned to the role

    - MS Windows OS uses this model with groups
- 5.4.2 Rule Based access control
    - A key characteristic of the Rule-Based access control model is that it applies global rules to all subjects
        - e.g. firewalls uses rules that allow or block traffic to all users equally
    - Rules within the rule-based access control model are sometimes referred to as restrictions or filters
- 5.4.3 Mandatory Access Control (MAC)
    - A key characteristic of the Mandatory Access Control (MAC) model is the use of labels applied to both subjects and objects
        - e.g. a label of top secret grants access to top-secret documents
    - When documented in a table, the MAC model sometimes resembles a lattice (i.e. climbing rosebush framework), so it is referred to as a lattice-based model
- 5.4.4 Discretionary Access Control (DAC)
    - A key characteristic of the Discretionary Access Control (DAC) model is that every object has an owner, and the owner can grant or deny access to any other subjects
        - e.g. you create a file and are the owner, and can grant permissions to that file
    - New Technology File System (NTFS) used in Windows, uses the DAC model
- 5.4.5 Attribute Based Access Control (ABAC)
    - A key characteristic of the Attribute-Based Access Control (ABAC) model is its use of rules that can include multiple attributes
        - this allows it to be much more flexible than a rule-based access control model that applies the rules to all subjects equally
        - many software-defined networks (SDNs) use the ABAC model
    - ABAC allows administrators to create rules within a policy using plain language statements such as “Allow Managers to access the WAN using a mobile device”
- 5.4.6 Risk based access control
    - Risk-based access control model grants access after evaluating risk; evaluating the environment and the situation and making risk-based decisions using policies embeded within software
        - Using machine learning, making predictive conclusions about current activity based on past activity

5.5 Manage the identity and access provisioning lifecycle (OSG-9 Chpts 13,14)

- 5.5.1 Account accesss review
    - Administrators need to periodically review user, system and service accounts to ensure they meet security policies and that they don’t have excessive privileges
    - Be careful in using the local system account as an application service account; although it allows the app to run without creating a special service account, it usually grants the app more access than it needs
    - You can use scripts to run periodically and check for unused accounts, and check priveleged group membership, removing unauthorized accounts
    - Guard against two access control issues:
        - excessive privilege: occurs when users have more privileges than assigned work tasks dictate; these privileges should be revoked
        - creeping privileges (AKA privilege creep): user accounts accumulating additional privileges over time as job roles and assigned tasks change

- 5.5.2 Provisioning and deprovisioning
    - Identity and access provisioning lifecycle refers to the creation, management, and deletion of accounts
        - this lifecycle is important because without properly defined and maintained user accounts, a system is unable to establish accurate identity, perform authentication, provide authorization, and track accountability
    - Provisioning/Onboarding
        - proper user account creation, or provisioning, ensures that personnel follow specific procedures when creating accounts
            - new-user account creation is AKA enrollment or registration
        - **automated provisioning**: information is provided to an app, that then creates the accounts via pre-defined rules (assigning to appropriate groups based on roles)
            - automated provisioning systems create accounts consistently
        - provisioning also includes issuing hardware, tokens, smartcards etc to employees
        - it's important to keep accurate records when issuing hardware to employees
        - after provisioning, an org can follow up with onboarding processes, including:
            - the employee reads and signs the acceptable use policy (AUP)
            - explaining security best practices (like infected emails)
            - reviewing the mobile device policy
            - ensuring the employee's computer is operational, and they can log in
            - configure a password manager
            - explaining how to access help desk
            - show to access, share and save resources
    - Deprovisioning/Offboarding
        - Deprovisioning/offboarding occurs when an employee leaves the organization or is transferred to a different department
        - **Account revocation**: deleting an account is the easiest way to deprovision
            - an employee's account is usually first disabled
            - supervisors can then review the user's data and determine if anything is needed
            - note: if terminated employee retains access to a user account after the exit interview, the risk for sabatage is very high
        - Deprovisioning includes collecting any hardware issued to an employee such as laptops, mobile devices and auth tokens
- 5.5.3 Role definition
    - Employee responsibilities can change in the form of transfers to a different role, or into a newly created role
        - for new roles, it's important to define the role and the privileges needed by the employees in that role
    - Roles and associated groups need to be defined in terms of privileges
- 5.5.4 Privilege escalation (e.g. managed service accounts, use of usdo, minimizing its use)
    - Privilege escalation refers to any situation that gives users more privileges than they should have
    - Attackers use privilege escalation techniques to gain elevated privileges
    - **Horizontal privilege escalation**: gives an attacker similar privileges as the first compromised user, but from other accounts
    - **Vertical privilege escalation**: provides an attacker with significantly greater privileges

        - e.g. after compromising a regular user's account an attacker can use vertical privilege escalation techniques to gain administrator privileges on the user's computer
        - the attacker can then use horizontal privilege escalation techniques to access other computers in the network
        - this horizontal privilege escalation throughout the network is AKA **lateral movement**

5.6 Implement authentication systems (OSG-9 Chpt 14)

- 5.6.1 OpenID Connect (OIDC) / Open Authorization (Oauth)
    - OAuth is an open framework used for authentication and authorization protocols
    - The most common protocol built on OAuth is OpenID Connect (OIDC)
    - OAuth 2.0 is often used for delegated access to applications, e.g. a mobile game that automatically finds all of your new friends from a social media app is likely using OAuth 2.0
    - Conversely, if you sign into a new mobile game using a social media account (instead of creating a user account just for the game), that process might use OIDC
    - **OpenID Connect (OIDC)**: an authentication layer using the OAuth 2.0 authorization framework, maintained by the OpenID Foundation, providing both authentication and authorization
    - OIDC uses JSON (JavaScript Object Notation) Web Tokens (JWT) -- AKA ID token
    - OAuth and OIDC are used with many web-based applications to share information without sharing credentials
        - OAuth provides authorization
        - OIDC uses the OAuth framework for authorization and builds on the OpenID technologies for authentication
- 5.6.2 Security Assertion Markup Language (SAML)
    - Security Assertion Markup Language (SAML): an open XML-based standard commonly used to exchange authentication and authorization (AA) information between federated orgs
    - SAML provides SSO capabilities for browser access
    - SAML is a popular SSO standard on the internet - used to exchange authentication and authorization (AA) information
    - Organization for the Advancement of Structure Information Standards (OASIS) maintains it
    - SAML 2 spec utilizes three entities:
        - Principal or User Agent
        - Service Provider (SP): providing the service a user is interested in using
        - Identity Provider (IdP): a third-party that holds the user authentication and authorization info
    - IdP can send three types of XML messages known as assertions:
        - Authentication Assertion: provides proof that the user agent provided the proper credentials, identifies the identification method, and identifies the time the user agent logged on
        - Authorization Assertion: indicates whether the user agent is authorized to access the requested service; if denied, includes why
        - Attribute Assertion: attributes can be any information about the user agent
- 5.6.3 Kerberos

- Kerberos is a network authentication protocol widely used in corporate and private networks and found in many LDAP and directory services solutions such as Microsoft Active Directory
- It provides single sign-on and uses cryptography to strengthen the authentication process
- The purpose of Kerberos is authentication; Kerberos offers a single sign-on solution for users and protects logon credentials
- Ticket authentication is a mechanism that employs a third-party entity to prove identification and provide authentication - Kerberos is a well-known ticket system
- After users authenticate and prove their identity, Kerberos uses their proven identity to issue tickets, and user accounts present these tickets when accessing resources
- Kerberos version 5 relies on symmetric-key cryptography (AKA secret-key cryptography) using the Advanced Encryption Standard (AES) symmetric encryption protocol
- Kerberos provides confidentiality and integrity for authentication traffic using end-to-end security and helps protect against eavesdropping and replay attacks
- Kerberos elements:
    - **Key Distribution Center (KDC)**: the trusted third party that provides authentication services
    - **Kerberos Authentication Server**: hosts the functions of the KDC:
        - **ticket-granting service (TGS)**: provides proof that a subject has authenticated through a KDC and is authorized to request tickets to access other objects
            - a TGT is encrypted and includes a symmetric key, an expiration time, and user's IP address
            - subjects present the TGT when requesting tickets to access objects
        - **authentication service (AS)**: verifies or rejects the authenticity and timeliness of tickets. Often referred to as the KDC
    - **ticket (AKA service ticket (ST))**: an encrypted message that provides proof that a subject is authorized to access an object
    - **Kerberos Principal**: typically a user but can be any entity that can request a ticket
    - **Kerberos realm**: a logical area (such as a domain or network) ruled by Kerberos
- Kerberos login process:
    - user types a username/password into the client
    - client encrypts the username with AES for transmission to the KDC
    - the KDC verifies the username against a db of known credentials
    - the KDC generates a symmetric key that will be used by the client and the Kerberos server
        - it encrypts this with a hash of the user's password
        - the KDC also generates an encrypted timestamped TGT
    - the KDC then transmits the encrypted symmetric key and the encrypted timestamped TGT to the client
    - the client installs the TGT for use until it expires
        - the client also decrypts the symmetric key using a hash of the user's password
        - NOTE: the client's password is never transmitted over the network, but it is verified
            - the server encrypts a symmetric key using a hash of the user's password, and it can only be decrypted with a hash of the user's password
            - as long as the user enters the correct password, this step works
- When a client wants to access an object (like a hosted resource), it must request a ticket through the Kerberos server, in the following steps:

        - the client sends its TGT back to the KDC with a request for access to the resource
        - the KDC verifies that the TGT is valid, and checks its access control matrix to verify user privileges for the requested resource
        - the KDC generates a service ticket and sends it to the client
        - the client sends the ticket to the server or service hosting the resource
        - the server or service hosting the resource verifies the validity of the ticket with the KDC
        - once identity and authorization are verified, Kerberos activity is complete
            - the server or service host then opens a session with the client and begins communication or data transmission

- 5.6.4 Remote Authentication Dial-in User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)

    - Remote Authentication Dial-in User Service (RADIUS): centralizes authentication for remote access connections, such as VPNs or dial-up access
        - a user can connect to any network access server, which then passes on the user's credentials to the RADIUS server to verify authentication and authorization and to track accounting
        - in this context, the network access server is the RADIUS client, and a RADIUS server acts as an authentication server
        - the RADIUS server also provides AAA services for multiple remote access servers
        - RADIUS uses the User Datagram Protocol (UDP) by default and encrypts only the password's exchange
        - RADIUS using Transport Layer Security (TLS) over TCP (port 2083) is defined by RFC 6614
        - RADIUS uses UDP port 1812 for RADIUS messages and UDP port 1813 for RADIUS Accounting messages
        - RADIUS encrypts only the password's exchange by default
        - it is possible to use RADIUS/TLS to encrypt the entire session
    - Cisco developed Terminal Access Control Access Control System Plus (TACACS+) and released it as an open standard
        - provides improvements over the earlier version and over RADIUS, it separates authentication, authorization, and accounting into separate processes, which can be hosted on three different servers
        - additionally, TACACS+ encrypts all of the authentication information, not just the password, as RADIUS does
        - TACACS+ uses TCP port 49, providing a higher level of reliability for the packet transmissions

Domain 6 **Security Assessment and Testing**

- Security assessment and testing programs are an important mechanism for validating the on-going effectiveness of security controls
    - they include a variety of tools, such as vulnerability assessments, penetration tests, software testing, audits, and other control validation
- Every org should have a security assessment and testing program defined and operational
- **Security assessments**: comprehensive reviews of the security of a system, application, or other tested environment

    - during a security assessment, a trained information security professional performs a risk assessment that identifies vulnerabilities in the tested environment that may allow a compromise and makes recommendations for remediation, as needed
    - a security assessment includes the use of security testing tools, but go beyond scanning and manual penetration tests
    - the main work product of a security assessment is normally an assessment report addressed to management that contains the results of the assessment in nontechnical language and concludes with specific recommendations for improving the security of the tested environment
- An organization's audit strategy will depend on its size, industry, financial status and other factors
    - a small non-profit, a small private company and a small public company will have different requirements and goals for their audit strategies
    - the audit strategy should be assessed and tested regularly to ensure that the organization is not doing a disservice to itself with the current strategy
    - there are three types of audit strategies: internal, external, and third-party

6.1 Design and validate assessment, test, and audit strategies (OSG-9 Chpt 15)

- 6.1.1 Internal
    - An organization's security staff can perform security tests and assessments, and the results are meant for internal use only, designed to evaluate controls with an eye toward finding potential improvements
    - An internal audit strategy should be aligned to the organization's business and day-to-day operations
        - e.g. a publicly traded company will have a more rigorous internal auditing strategy than a privately held company
    - Designing the audit strategy should include laying out applicable regulatory requirements and compliance goals
    - Internal audits are performed by an organization's internal audit staff and are typically intended for internal audiences
- 6.1.2 External
    - An external audit strategy should complement the internal strategy, providing regular checks to ensure that procedures are being followed and the organization is meeting its compliance goals
    - External audits are performed by an outside auditing firm
        - these audits have a high degree of external validity because the auditors performing the assessment theoretically have no conflict of interest with the org itself
        - audits by these firms are generally considered acceptable by most investors and governing bodies
- 6.1.3 Third-party
    - Third-party audits are conducted by, or on behalf of, another org
    - In the case of a third-party audit, the org initiating the audit generally selects the auditors and designs the scope of the audit
    - The statement on **Standards for Attestation Engagements document 18 (SSAE 18)**, titled Reporting on Controls, provides a common standard to be used by auditors performing assessments of service orgs

with the intent of allowing the org to conduct external assessments, instead of multiple third-party assessments, and then sharing the resulting report with customers and potential customers
        - outside of the US, similar engagements are conducted under the International Standard for Attestation Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization
    - SSAE 18 and ISAE 3402 engagements are commonly referred to as a service organization controls (SOC) audits
    - Three forms of SOC audits:
        - **SOC 1 Engagements**: assess the organization's controls that might impact the accuracy of financial reporting
        - **SOC 2 Engagements**: assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system
            - SOC 2 audit results are confidential and are usually only shared outside an org under an NDA
        - **SOC 3 Engagements**: assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy information stored in a system
            - however, SOC3 audit results are intended for public disclosure
    - Two types of SOC reports:
        - **Type I Reports**: provide the auditor's opinion on the description provided by management and the suitability of the design of the controls
            - type I reports also cover only a specific point in time, rather than an extended period
            - think of Type I report as more of a documentation review
        - **Type II Reports**: go further and also provide the auditor's opinion on the operating effectiveness of the controls
            - the auditor actually confirms the controls are functioning properly
            - Type II reports also cover an extended period of time, at least 6 months
            - think of Type II report as similar to a traditional audit; the auditor is checking the paperwork, and verifying the controls are functioning properly
        - Type II reports are considered much more reliable than Type I reports (Type I reports simply take the service orgs word that the controls are implemented as described)

6.2 Conduct security control testing (OSG-9 Chpt 15)

- Security control testing can include testing of the physical facility, logical systems and applications; common testing methods:

- 6.2.1 Vulnerability assessment

    - **Vulnerabilities**: weaknesses in systems and security controls that might be exploited by a threat
    - Vulnerability assessments: examining systems for these weaknesses
    - The goal of a vulnerability assessment is to identify elements in an environment that are not adequately protected -- and not necessarily from a technical perspective; you can also assess the vulnerability of physical security or the external reliance on power, for instance
        - can include personnel testing, physical testing, system and network testing, and other facilities tests

- Vulnerability assessments are some of the most important testing tools in the information security professional's toolkit
- **Security Content Automation Protocol (SCAP)**: provides a common framework for discussion and facilitation of automation of interactions between different security systems (sponsored by NIST)
    - SCAP components related to vulnerability assessments:
        - **Common Vulnerabilities and Exposures (CVE)**: provides a naming system for describing security vulnerabilities
        - **Common Vulnerability Scoring Systems (CVSS)**: provides a standardized scoring system for describing the severity of security vulnerabilities
        - **Common Configuration Enumeration (CCE)**: provides a naming system for system config issues
        - **Common Platform Enumeration (CPE)**: provides a naming system for operating systems, applications, and devices
        - **Extensible Configuration Checklist Description Format (XCCDF)**: provides a language for specifying security checklists
        - **Open Vulnerability and Assessment Language (OVAL)**: provides a language for describing security testing procedures
- Vulnerability scans automatically probe systems, applications, and networks looking for weaknesses that could be exploited by an attacker
- Four main categories of vulnerability scans:
    - network discovery scans
    - network vulnerability scans
    - web application vulnerability scans
    - database vulnerability scans

- 6.2.2 Penetration testing

    - Penetration tests goes beyond vulnerability testing techniques because it actually attempts to exploit systems
    - NIST defines the penetration testing process as consisting of four phases:
    - **planning**: includes agreement on the scope of the test and the rules of engagement
        - ensures that both the testing team and management are in agreement about the nature of the test and that it is explicitly authorized
    - **information gathering and discovery**: uses manual and automated tools to collect information about the target environment
        - basic reconnaissance (website mapping)
        - network discovery
        - testers probe for system weaknesses using network, web and db vuln scans
    - **attack**: seeks to use manual and automated exploit tools to attempt to defeat system security
        - step where pen testing goes beyond vuln scanning as vuln scans don't attempt to actually exploit detected vulns
    - **reporting**: summarizes the results of the pen testing and makes recommendations for improvements to system security
    - tests are normally categorized into three groups:

        - **white-box penetration test**:
            - provides the attackers with **detailed information** about the systems they target
            - this bypasses many of the reconnaissance steps that normally precede attacks, shortening the time of the attack and increasing the likelihood that it will find security flaws
            - these tests are sometimes called "**known environment**" tests
        - **gray-box penetration test**:
            - AKA **partial knowledge tests**, these are sometimes chosen to balance the advantages and disadvantages of white- and black-box penetration tests
            - this is particularly common when black-box results are desired but costs or time constraints mean that some knowledge is needed to complete the testing
            - these tests are sometimes called "**partially known environment**" tests
        - **black-box penetration test**:
            - does not provide attackers with any information prior to the attack
            - this simulates an external attacker trying to gain access to information about the business and technical environment before engaging in an attack
            - these tests are sometimes called "**unknown environment**" tests

- 6.2.3 Log reviews

    - **Security Information and Event Management (SIEM)**: packages that collect information using the syslog functionality present in many devices, operating systems, and applications
    - Admins may choose to deploy logging policies through Windows Group Policy Objects (GPOs)
    - Logging systems should also make use of the Network Time Protocol (NTP) to ensure that clocks are synchronized on systems sending log entries to the SIEM as well as the SIEM itself, ensuring info from multiple sources have a consistent timeline
    - Information security managers should also periodically conduct log reviews, particularly for sensitive functions, to ensure that privileged users are not abusing their privileges
    - Network flow (NetFlow) logs are particularly useful when investigating security incidents

- 6.2.4 Synthetic transactions

    - **Synthetic transactions**: scripted transactions with known expected results
    - Dynamic testing may include the use of synthetic transactions to verify system performance; synthetic transactions are run against code and compare out to expected state

- 6.2.5 Code review and testing

    - Code review and testing is "one of the most critical components of a software testing program"
    - These procedures provide third-party reviews of the work performed by developers before moving code into a production environment, possibly discovering security, performance, or reliability flaws in apps before they go live and negatively impact business operations
    - In code review, AKA peer review, developers other than the one who wrote the code review it for defects
    - **Fagan inspections**: the most formal code review process follows six steps:
        1. planning
        2. overview
        3. preparation

4. inspection
5. rework
6. follow-up

- **Static application security testing (SAST)**: evaluates the security of software without running it by analyzing either the source code or the compiled application
- **Dynamic application security testing (DAST)**: evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else

- 6.2.6 Misuse case testing

  - **Misuse case testing**: AKA abuse case testing - used by software testers to evaluate the vulnerability of their software to known risks
  - In misuse case testing, testers first enumerate the known misuse cases, then attempt to exploit those use cases with manual or automated attack techniques

- 6.2.7 Test coverage analysis

  - A test coverage analysis is used to estimate the degree of testing conducted against new software
  - **Test coverage** = number of use cases tested / total number of use cases
    - requires enumerating possible use cases (which is a difficult task), and anyone using test coverage calcs to understand the process used to develop the input values
  - Five common criteria used for test coverage analysis:
    - **branch coverage**: has every IF statement been executed under all IF and ELSE conditions?
    - **condition coverage**: has every logical test in the code been executed under all sets of inputs?
    - **functional coverage**: has every function in the code been called and returned results?
    - **loop coverage**: has every loop in the code been executed under conditions that cause code execution multiple times, only once, and not at all?
    - **statement coverage**: has every line of code been executed during the test?

- 6.2.8 Interface testing

  - Interface testing assesses the performance of modules against the interface specs to ensure that they will work together properly when all the development efforts are complete
  - Three types of interfaces should be tested:
    - application programming interfaces (APIs): offer a standardized way for code modules to interact and may be exposed to the outside world through web services
      - should test APIs to ensure they enforce all security requirements
    - user interfaces (UIs): examples include graphical user interfaces (GUIs) and command-line interfaces
      - UIs provide end users with the ability to interact with the software, and tests should include reviews of all UIs
    - physical interfaces: exist in some apps that manipulate machinery, logic controllers, or other objects
      - software testers should pay careful attention to physical interfaces because of the potential consequences if they fail

- 6.2.9 Breach attack simulations
    - **Breach and attack simulation (BAS)**: platforms that seek to automate some aspects of penetration testing
    - The BAS platform is not actually waging attacks, but conducting automated testing of security controls to identify deficencies
    - Designed to inject threat indicators onto systems and networks in an effort to trigger other security controls (e.g. place a suspicious file on a server)
        - detection and prevention controls should immediately detect and/or block this traffic as potentially malicious
    - See:
        - OWASP Web Security Testing Guide
        - OSSTMM (Open Source Security Testing Methodology Manual)
        - NIST 800-115
        - FedRAMP Penetration Test Guidance
        - PCI DSS Information Supplemental on Penetration Testing
- 6.2.10 Compliance checks
    - Orgs should create and maintain compliance plans documenting each of their regulatory obligations and map those to the specific security controls designed to satisfy each objective
    - Compliance checks are an important part of security testing and assessment programs for regulated firms: these checks verify that all of the controls listed in a compliance plan are functioning properly and are effectively meeting regulatory requirements

6.3 Collect security process data (e.g. technical and administrative) (OSG-9 Chpts 15,18)

- 6.3.1 Account management
    - Preferred attacker techniques for obtaining privilege user access include:
        - compromising an existing privileged account: mitigated through use of strong authentication (strong passwords and multifactor), and by admins use of privileged accounts only for specific tasks
        - privelege escalation of a regular account or creation of a new account: these approaches can be mitigated by paying attention to the creation, modification, and use of user accounts
- 6.3.2 Management review and approval
    - Account management reviews ensure that users only retain authorized permissions and that unauthorized modifications do not occur
    - Full review of accounts: time-consuming to review all, and often done only for highly privileged accounts
    - Organizations that don't have time to conduct a full review process may use sampling, but only if sampling is truely random
    - Adding accounts: should be a well-defined process, and users should sign AUP
    - Adding, removing, and modifying accounts and permissions should be carefully controlled and documented
    - Accounts that are no longer needed should be suspended

    - ISO 9000 standards use a Plan-Do-Check-Act loop
        - plan: foundation of everything in the ISMS, determines goals and drives policies
        - do: security operations
        - check: security assessment and testing (this objective)
        - act: formally do the management review

- 6.3.3 Key performance and risk indicators

    - **Key Performance Indicator (KPIs)**: measures that provide significance of showing the performance an ISMS compared to stated goals
    - Choose the factors that can show the state of security
    - Define baselines for some (or better yet all) of the factors
    - Develop a plan for periodically capturing factor values (use automation!)
    - Analyze and interpret the data and report the results
    - Key metrics or KPIs that should be monitored by security managers may vary from org to org, but could include:
        - number of open vulns
        - time to resolve vulns
        - vulnerability/defect recurrence
        - number of compromised accounts
        - number of software flaws detected in pre-production scanning
        - repeat audit findings
        - user attempts to visit known malicious sites
    - Develop a dashboard of metrics and track them

- 6.3.4 Backup verification data

    - Managers should periodically inspect the results of backups to verify that the process functions effectively and meets the organization's data protection needs
        - this might include reviewing logs, inspecting hash values, or requesting an actual restore of a system or file

- 6.3.5 Training and awareness

    - Training and awareness programs play a crucial role in preparing an organization's workforce to support information security programs
    - They educate employees about current threats and advise them on best practices for protecting information and systems under their care from attacks
    - Program should begin with initial training designed to provide foundation knowledge to employees who are joining the org or moving to a new role; the initial training should be tailored to an individual's role
    - Training and awareness should continue to take place throughout the year, reminding employees of their responsibilities and updating them on changes to the organization's operating environment and threat landscape
    - Use phishing simulations to evaluate the effectiveness of their security awareness programs

- 6.3.6 Disaster Recover (DR) and Business Continuity (BC)

    - **Business Continuity (BC)**: the processes used by an organization to ensure, holistically, that its vital business processes remain unaffected or can be quickly restored following a serious incident
    - **Disaster Recovery (DR)**: is a subset of BC, that focuses on restoring information systems after a disaster
    - These processes need to be periodically accessed, and regular testing of disaster recovery and business continuity controls provide organizations with the assurance they are effectively protected against disruptions to business ops
    - Protection of life is of the utmost importance and should be dealt with first before attempting to save material things

6.4 Analyze test output and generate report (OSG-9 Chpt 15)

- Step 1: review and understand the data
    - The goal of the analysis process is to proceed logically from facts to actionable info
    - A list of vulns and policy exceptions is of little value to business leaders unless it's used in context, so once all results have been analyzed, you're ready to start writing the official report
- Step 2: determine the business impact of those facts
    - Ask "so what?"
- Step 3: determine what is actionable
    - The analysis process leads to valuable results only if they are actionable
- 6.4.1 Remediation
    - Rather than software defects, most vulnerabilities in average orgs come from misconfigured systems, inadequate policies, unsound business processes, or unaware staff
    - Vuln remediation should include all stakeholders, not just IT
- 6.4.2 Exception handling
    - **Exception handling**: the process of handling unexpected activity, since software should never depend on users behaving properly
        - "expect the unexpected", gracefully handle invalid input and improperly sequenced activity etc
    - Sometimes vulns can't be patched in a timely manner (e.g. medical devices needing re-accreditation) and the solution is to implement compensitory controls, document the excpetion and decision, and revisit
        - **compensitory controls**:measures taken to address any weaknesses of existing controls or to compensate for the inability to meet specific security requirements due to various different constraints
        - e.g. micro-segmentation of device, access restrictions, monitoring etc
    - Exception handling may be required due to system crash as the result of patching (requiring roll-back)
- 6.4.3 Ethical disclosure
    - While conducting security testing, cybersecurity pros may discover previously undiscovered vulns (perhaps implementing compensating controls to correct) that they may be unable to correct

- **Ethical disclosure**: the idea that security pros who detect a vuln have a responsibility to report it to the vendor, providing them with enough time to patch or remediate
    - the disclosure should be made privately to the vendor providing reasonable amount of time to correct
    - if the vuln is not corrected, then public disclosure of the vuln is warrented, such that other professionals can make informed decisions about future use of the product(s)

6.5 Conduct or facilitate security audits (OSG-9 Chpt 15)

- 6.5.1 Internal
    - Having an internal team conduct security audits has several advantages:
        - understanding of the internal environment reduces time
        - an internal team can delve into all parts of systems, because they have insider knowledge
        - internal auditors can be more agile in adapting to changing needs, rescheduling failed assessment components quickly
    - Disadvantages of using an internal team to conduct security audits:
        - the team may have limited exposure to new/other methodologies (e.g. the team may have depth but not breadth of experience and knowledge)
        - potential conflicts of interest (e.g. reluctance to throw other teams under the bus and accurately report their findings)
        - audit team members may start with an agenda (say to secure funding) and overstate faults, or have interpersonal motives
- 6.5.2 External
    - An external audit (sometimes called a second-party audit) is one conducted by (or on behalf of) a business partner
    - External audits are tied to contracts; by definition, an external audit should be scoped to include only the contractual obligations of an organization
- 6.5.3 Third-party
    - Third-party audits are often needed to demonstrate compliance with some government regulation or industry standard
    - Advantages of having a third-party audit an organization:
        - they likely have breadth of experience auditing many types of systems, across many types of organizations
        - they are not affected by internal dynamics or org politics
    - Disadvantage of using a third-party auditor:
        - cost: third-party auditors are going to be much more costly than internal teams; this means that the organization is likely to conduct audits as frequently
        - internal resources are still required to assist or accompany auditors, to answer questions and guide

Domain 7 **Security Operations**

7.1 Understand and comply with investigations (OSG-9 Chpt 19)

- **Investigation**: a formal inquiry and systematic process that involves gathering information to determine the cause of a security incident or violation

- Investigators must be able to conduct reliable investigations that will hold up in court; securing the scene is an essential and critical part of every investigation

    - securing the scene might include any/all of the following:
        - sealing off access to the area or crime scene
        - taking images of the scene
        - documenting evidence
        - ensuring evidence (e.g. computers, mobile devices, portable drives etc) is not contacted, tampered with, or destroyed
    - general principles:
        - identify and secure the scene
        - protect evidence -- proper collection of evidence preserves its integrity and the chain of custody
        - identification and examination of the evidence
        - further analysis of the most compelling evidence
        - final reporting of findings

- **Locard exchange principle**: whenever a crime is commited something is taken, and something is left behind

- The purpose of an investigation is to:

    - identify the root cause of the incident
    - prevent future occurrences
    - mitigate the impact of the incident on the organization

- Types of investigations:

    - **administrative**: an investigation that is focused on policy violations
    - **criminal**: conducted by law enforcement, this type of investigation tries to determine if there is cause to believe (beyond a reasonable doubt) that someone committed a crime
        - the goal is to gather evidence that can be used to convict in court
        - the job of a security professional is to preserve evidence, ensure law enforcement has been contacted, and assist as necessary
    - **civil**: non-criminal investigation for matters such as contract disputes
        - the goal of a civil investigation is to gather evidence that can be used to support a legal claim in court, and is typically triggered from an imminent or on-going lawsuit
        - the level of proof is much lower for a civil compared to a criminal investigation
    - **regulatory**: investigation initiated by a government regulator when there is reason to believe an organization is not in compliance
        - this type of investigation varies significantly in scope and could look like any of the other three types of investigation depending on the severity of the allegations

        - as with criminal investigations, it is key to preserve evidence, and assist the regulator's investigators

- 7.1.1 Evidence collection and handling

    - Evidence collection is complex, should be done by professionals, and can be thrown out of court if incorrectly handled
    - It's important to preserve original evidence
    - International Organization on Computer Evidence (IOCE) six principles for media, network and software analysis:
        - all general forensic and procedural principles must be applied to digital evidence collection
        - seizing digital evidence shouldn't change the evidence
        - accessing original digital evidence should only be done by trained professionals
        - all activity relating to seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review
        - a person in possession of digital evidence is responsible for all actions taken with respect to that evidence
        - any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles
    - Scientific Working Group on Digital Evidence (SWGDE) developed principles for standardized recovery of computer-based evidence:
        - legal system consistency
        - use of a common language
        - durability
        - ability to cross international and state boundaries
        - instill confidence in evidence integrity
        - forensic evidence applicability at the individual, agency, and country levels
    - **ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence**: the international standard on digital evidence handling, with four phases:
        - identification
        - collection
        - acquisition
        - preservation
    - Types of evidence:
        - **primary evidence**:
            - most reliable and used at trial
            - original documents (e.g. legal contracts), no copies or duplicates
        - **secondary evidence**:
            - less powerful and reliable than primary evidence (e.g. copies of originals, witness oral evidence etc)
            - if primary evidence is available secondary of the same content is not valid
        - **real evidence**: this type of evidence includes physical objects, such as computers, hard drives, and other storage devices, that can be brought into a court of law

        - **direct evidence**: this type of evidence is based on the observations of a witness or expert opinion and can be used to prove a fact at hand (with backup evidence support)
        - **circumstantial evidence**: this type of evidence is based on inference and can be used to support a conclusion, but not prove it
        - **corroborative evidence**: this type of evidence is used to support other evidence and can be used to strengthen a case
        - **hearsay evidence**: type of evidence that is based on statements made by someone outside of court and is generally not admissible
        - **best evidence rule**: states that the original evidence should be presented in court, rather than a copy or other secondary evidence
    - It is important to note that evidence should be collected and handled in a forensically sound manner to ensure that it is admissible in court and to avoid any legal issues
    - The chain of custody: focuses on having control of the evidence -- who collected and handled what evidence, when, and where
        - think about establishing the chain of custody as:
            - tag,
            - bag, and
            - carry the evidence
    - Five rules of evidence: five evidence characteristics providing the best chance of surviving legal and other scrutiny:
        - **authentic**: evidence is not fabricated or planted, and can be proven through crime scene photos, or bit-for-bit copies of storage
        - **accurate**: evidence that has integrity (not been modified)
        - **complete**: evidence must be complete, and all parts available and shared, whether they support the case or not
        - **convincing**: evidence must be easy to understand, and convey integrity
        - **admissible**: evidence must be accepted as part of a case

- 7.1.2 Reporting and documentation

    - Each investigation should result in a final report that documents the goals of the investigation, the procedures followed, the evidence collected, and the final results
    - Preparing formal documentation prepares for potential legal action, and even internal investigations can become part of employment disputes
    - Identify in advance a single point of contact who will act as your liasion with law enforcement, providing a go-to person with a single perspective, potentially improving the working relationship
    - Participate in the FBI's InfraGard program

- 7.1.3 Investigative techniques

    - Whether in response to a crime or incident, an organizational policy breach, troubleshooting a system or network issue etc, digital forensic methodologies can assist in finding answers, solving problems, and in some cases, help in successfully prosecuting crimes
    - The forensic investigation process should include the following:
        - identification and securing of a crime scene

        - proper collection of evidence that preserves its integrity and the chain of custody
        - examination of all evidence
        - further analysis of the most compelling evidence
        - final reporting
    - Sources of information and evidence:
        - oral/written statements: given to police, investigators, or as testimony in court by people who witness a crime or who may have pertient information
        - written documents: checks, printed contracts, handrwitten letters/notes
        - computer systems: components, local/portable storage, memory etc
        - visual/audio: visual and audio evidence pertient to a security investigation could include photographs, video, taped recordings, and surveillance footage from security cameras
    - Several investigative techniques can be used when conducting analysis:
        - media analysis: examining the bits on a hard drive that are intact dispite not having an index
        - software analysis: focuses on an applications and malware, determining how it works and what it's trying to do, with a goal of attribution

- 7.1.4 Digital forensics tools, tactics, and procedures

    - Digital forensics: the scientific examination and analysis of data from storage media so that the information can be used as part of an investigation to identify the culprit or the root cause of an incident
    - **Live evidence**: data stored in a running system e.g. random access memory (RAM), cache, and buffers
    - Examining a live system can change the state of the evidence
        - small changes like interacting with the keyboard, mouse, loading/unloading programs, or of course powering off the system, can change or eliminate live evidence
    - Whenever a forensic investigation of a storage drive is conducted, two identical bit-for-bit copies of the original drive should be created first
    - **eDiscovery**: the process of identifying, collecting, and producing electronic evidence in legal proceedings

- 7.1.5 Artifacts (e.g. computer, network, mobile device)

    - Forensic artifacts: remnants of a system or network breach/attempted breach, which and may or may not be relevant to an investigation or response
    - Artifacts can be found in numerous places, including:
        - computer systems
        - web browsers
        - mobile devices
        - hard drives, flash drives

7.2 Conduct logging and monitoring activities (OSG-9 Chpts 17,21)

- 7.2.1 Intrusion detection and prevention
- 7.2.2 Security Information and Event Management (SIEM)
    - Security Information and Event Management (SIEM): systems that ingest logs from multiple sources, compile and analyze log entries, and report relevant information
        - SIEM systems are complex and require expertise to install and tune

        - require a properly trained team that understands how to read and interpret info, and escalation procedures to follow when a legitimate alert is raised
        - SIEM systems represent technology, process, and people, and each is important to overall effectiveness
        - a SIEM includes significant intelligence functionality, allowing large amounts of logged events and analysis and correlation of the same to occur very quickly
    - SIEM capabilities include:
        - Aggregation
        - Normalization
        - Correlation
        - Secure storage
        - Analysis
        - Reporting
- 7.2.3 Continuous monitoring
- 7.2.4 Egress monitoring
- 7.2.5 Log management
- 7.2.6 Threat intelligence (e.g. threat feeds, threat hunting)
- 7.2.7 use and Entity Behavior Analytics (UEBA)

7.3 Perform Configuration Management (CM) (e.g. provisioning, baselining, automation) (OSG-9 Chpt 16)

7.4 Apply foundational security operations concepts (OSG-9 Chpt 16)

- 7.4.1 Need-to-know/least privilege
- 7.4.2 Separation of Duties (SoD) and responsibilities
- 7.4.3 Privilege account management
- 7.4.4 Job rotation
- 7.4.5 Service Level Agreements (SLA)

7.5 Apply resource protection (OSG-9 Chpt 16)

- 7.5.1 Media management
- 7.5.2 Media protection techniques

7.6 Conduct incident management (OSG-9 Chpt 17)

- 7.6.1 Detection
- 7.6.2 Response
- 7.6.3 Mitigation
- 7.6.4 Reporting
- 7.6.5 Recovery
- 7.6.6 Remediation
- 7.6.7 Lessons Learned

7.7 Operate and maintain detective and preventative measures (OSG-9 Chpts 11,17)

- 7.7.1 Firewalls (e.g. next generation, web application, network)

- 7.7.2 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- 7.7.3 Whitelisting/blacklisting
- 7.7.4 Third-party provided security services
- 7.7.5 Sandboxing
- 7.7.6 Honeypots/honeynets
- 7.7.7 Anti-malware
- 7.7.8 Machine learning and Artificial Intelligence (AI) based tools

7.8 Implement and support patch and vulnerability management (OSG-9 Chpt 16)

7.9 Understand and participate in change management processes (OSG-9 Chpt 16)

7.10 Implement recovery strategies (OSG-9 Chpt 18)

- 7.10.1 Backup storage strategies
- 7.10.2 Recovery site strategies
- 7.10.3 Multiple processing sites
- 7.10.4 System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance

7.11 Implement Disaster Recovery (DR) processes (OSG-9 Chpt 18)

- 7.11.1 Response
- 7.11.2 Personnel
- 7.11.3 Communications
- 7.11.4 Assessment
- 7.11.5 Restoration
- 7.11.6 Training and awareness
- 7.11.7 Lessons learned

7.12 Test Disaster Recovery Plans (DRP) (OSG-9 Chpt 18)

- 7.12.1 Read-through/tabletop
- 7.12.2 Walkthrough
- 7.12.3 Simulation
- 7.12.4 Parallel
- 7.12.5 Full interruption

7.13 Particpate in Business Continuity (BC) planning and exercises (OSG-9 Chpt 3)

7.14 Implement and manage physical security (OSG-9 Chpt 10)

- 7.14.1 Perimeter security controls
- 7.14.2 Internal security controls

7.15 Address personnel safety and security concerns (OSG-9 Chpt 16)

- 7.15.1 Travel
- 7.15.2 Security training and awareness

- 7.15.3 Emergency management
- 7.15.4 Duress

Domain 8 **Software Development Security**

8.1 Understand and integrate security in the Software Develoment Life Cycle (SDLC)

8.2 Identify and apply security controls in software development ecosystems

8.3 Assess the effectiveness of software security

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards