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. 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
- **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 designed for critical infrastructure and commercial organizations, whereas the RMF establishes manditory requirements for federal agencies
  - The RMF, defined by NIST in SP 800-37 Rev 2, establishes manditory security requirements for federal agencies
  - There are other risk frameworks, such as the British Standard BS 31100. Be familiar with frameworks and their goals
  - 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

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 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, 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, 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.