Hi, I'm Mike Chapple, one of the authors of the official CISSP study guide. In this series of audio reviews, I'm going to walk you through the study essentials from each chapter in a convenient audio format that you can use to help you prepare for the exam. You might want to listen to these reviews after you've read each chapter. Use them in the car, at the gym or wherever it's convenient for you.

Let's take a look at the study essentials for chapter 1, security governance through principles and policies. You need to understand the CIA triad elements of confidentiality, integrity and availability. Confidentiality is the principle that objects are not disclosed to unauthorized subjects. Integrity is the principle that objects retain their veracity and are intentionally modified only by authorized subjects and availability is the principle that authorized subjects are granted timely and uninterrupted access to objects. You need to know the elements of AAA services. AAA services focus on identification, authentication, authorization, auditing and accounting.

Be able to explain how identification works. Identification is one of a subject professes an identity and accounting is initiated. A subject must provide an identity to a system to start the process of authentication, authorization and accounting. Understand the process of authentication. Authentication is the process of verifying or testing that a claimed identity is valid. Authentication requires information from the subject that must exactly correspond to the identity indicated. Know how authorization fits into a security plan. Once a subject is authenticated, it's access must be authorized. The process of authorization ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity.

Be able to explain the auditing process. Auditing is the programmatic means by which subjects are held accountable for their actions, while authenticated on a system through the documentation or recording of subject activities. Understand the importance of accounting. Security can be maintained only if subjects are held accountable for their actions. Effective accounting relies on the capability to prove a subject's identity and track their activities. Be able to explain the concept of abstraction. Abstraction is used to collect similar elements into groups, classes or roles that are assigned security controls, restrictions or permissions as a collective. It adds efficiency to carrying out a security plan.

Know about security boundaries. A security boundary is the line of intersection between any two areas, subnets or environments that have different security requirements or needs. Understand security governance. Security governance is the collection of practices related to supporting, defining and directing the security efforts of an organization. Know about third-party governance. Third-party governance is a system of external entity oversight that maybe mandated by law, regulation, industry standards, contractual obligation or licensing requirements. The actual method of governance may vary, but it generally involves an outside investigator or auditor.

Understand documentation review. Documentation review is the process of reading the exchange materials and verifying them against standards and expectations. In many situations, especially those related to government or military agencies or contractors, failing to provide sufficient documentation to meet the requirements of third-party governance can result in a loss of or avoiding of authorization to operate ATO. Understand the alignment of the security function to business strategy, goals, mission and objectives. Security management planning ensures the proper creation, implementation and enforcement of a security policy. Security management planning aligns the security functions with the strategy, goals, mission and objectives of the organization. This includes designing and implementing security based on business cases, budget restrictions or scarcity of resources.

Know what a business case is. A business case is usually a documented argument or stated position in order to define a need to make a decision or take some form of action. To make a business case is to demonstrate a business specific need to alter an existing process or choose an approach to a business task. A business case is often made to justify the start of a new project, especially a project

related to security. Understand security management planning. Security management is based on three types of plans, strategic, tactical and operational. A strategic plan is a long-term plan that is fairly stable. It defines the organization's goals, mission and objectives. The tactical plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. Operational plans are short term and highly detailed plans based on strategic and tactical plans.

Know the elements of a formalized security policy structure. To create a comprehensive security plan, you need the following items in place. Security policy, standards, baselines, guidelines and procedures. Understand key security roles. The primary security roles are senior manager, security professional, asset owner, custodian, user and auditor. Understand due diligence and due care. Due diligence is establishing a plan, policy and process to protect the interests of the organization. Due care is practicing the individual activities that maintain the due diligence effort. Due diligence is knowing what should be done and planning for it. Due care is doing the right action at the right time. Know the basics of threat modeling. Threat modeling is the security process where potential threats are identified, categorized and analyzed. Threat modeling can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed.

Key concepts here include assets attackers and software, STRIDE, PASTA, VAST, diagramming, reduction in decomposition and threat. Understand supply chain risk management concepts. Supply chain risk management or SCRM is a means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners. SCRM includes evaluating risks associated with hardware, software and services, performing third-party assessment and monitoring, establishing minimum security requirements and enforcing service level requirements. Those are the study essentials that you'll need to know for chapter 1, security governance through principles and policies.