Hi, I'm Mike Chapple and this is the audio review of the exam essentials for chapter 14 of the official CISSP study guide. Here are the top things you need to know for the exam from this chapter on controlling and monitoring access.

Identify common authorization mechanisms. Authorization ensures that the requested activity or object access is possible given the authenticated identity's privileges. For example, it ensures that users with appropriate privileges can access files and other resources. Common authorization mechanisms include implicit deny, access control lists, access control matrices, capability lists, constrained interfaces, content dependent controls and context dependent controls. These mechanisms enforce security principles such as need to know, the principle of least privilege and separation of duties.

Describe key concepts of the discretionary access control DAC model. With the DAC model, all objects have owners and the owners can modify permissions. Each object has an access control list defining permissions such as read and modify for files. All other models are non-discretionary models and administrators centrally manage non-discretionary controls.

Describe key concepts of the role-based access control model. Role-based access control, or RBAC models use job roles and users gain privileges when administrators place their accounts into a role or group. Taking a user out of a role removes the permissions granted through the role membership.

Describe key concepts of the rule-based access control model. Rule-based access control models use a set of rules, restrictions or filters to determine access. A firewall's access control list includes a list of rules that define what access is allowed and what access is blocked.

Describe key concepts of the attribute-based access control ABAC model. An ABAC model is an advanced implementation of a rule-based access control model applying rules based on attributes. Software defined networks or SDNs often use an ABAC model.

Describe key concepts of the mandatory access control or MAC model. The MAC model uses labels to identify security domains. Subjects need matching labels to access objects. The MAC model enforces the need to know principle and supports a hierarchical environment, a compartmentalized environment or a combination of both in a hybrid environment. MAC is frequently referred to as a lattice-based model.

Describe key concepts of the risk-based access control model. A risk-based access control model evaluates the environment and the situation and makes decisions based on software-based security policies. It can control access based on multiple factors such as the user's location determined by IP addresses, whether the user has logged on with multifactor authentication and the user's device. Advanced implementations can use machine learning to evaluate risk.

Understand single sign-on methods used on the internet. SSO is a mechanism that allows subjects to authenticate once and access multiple objects without authenticating again. Security assertion markup language or SAML is an open XML based standard used to exchange authentication and authorization information. OAuth 2.0 is an authorization framework described in RFC 6749 and supported by many online sites. Oasis maintains OpenID Connect OIDC. OIDC provides both authentication and authorization by using the OAuth 2.0 framework and building on the OpenID standard.

Describe Kerberos. Kerberos is the most common single sign-on method used within organizations. The primary purpose of Kerberos is authentication. It uses symmetric cryptography and tickets to prove identification and provide authentication. One server synchronizes it's time with a network time

protocol NTP server and all clients within a network synchronize with that same time. Understand the purpose of AAA protocols. Several protocols provide centralized authentication, authorization and accounting services. Network access or remote access systems use AAA protocols. For example, a network access server is a client to a radius server and the radius server provides AAA services. Radius uses UDP and encrypts the password only. TACACS plus uses TCP and encrypts the entire session.

Describe privilege escalation. Attackers use privilege escalation techniques to gain additional privileges after exploiting a single system. They typically try to gain additional privileges on the exploited systems first. They can also reach other systems in a network and attempt to gain elevated privileges on them. Limiting privileges given the service accounts reduces the success of some privilege escalation attacks.

Explain zero trust principles. Zero trust presumes that there is no trust boundary and no network edge. Instead, each action is validated when requested as part of a continuous authentication process and access is only allowed after policies are checked. The key components of a zero trust architecture are the policy engine and policy administrator, which together are known as the policy decision point and the policy enforcement point.

Know about Kerberos exploitation attacks. Kerberos attacks attempt to exploit weaknesses in Kerberos tickets. In some attacks, They capture tickets held in the LSASS.exe process and use them and pass the ticket attacks. A silver ticket grants the attacker all the privileges granted to a service account. Attackers can create golden tickets after obtaining the hash of the Kerberos service account, giving them the ability to create tickets at will within active directory.

Know how brute force and dictionary attacks work. Brute force and dictionary attacks are carried out against a stolen password database file or the system's log on prompt. They're designed to discover passwords. In brute-force attacks, all possible combinations of keyboard characters are used, whereas a predefined list of possible passwords is used in a dictionary attack. Account lockout controls limit the effectiveness of these attacks. Those are the study essentials that you need to know for Chapter 14, controlling and monitoring access.