Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 13 of the official CISSP study guide. Here are the top things you need to know from this chapter on managing identity and authentication.

Know how physical access controls protect assets. Physical access controls are those you can touch and they directly protect systems, devices and facilities by controlling access and controlling the environment. Indirectly, they also protect information and applications by limiting physical access. Know how logical access controls protect assets. Logical access controls include authentication, authorization and permissions. They limit who can access information, settings and use of information systems, devices, facilities, applications and services.

Know the difference between subjects and objects. You'll find that security documentation commonly uses the term subject and object, so it's important to know the difference between them. Subjects are active entities such as users that access passive objects such as files. A user is a subject who accesses objects while performing some action or accomplishing a work task.

Know the components of the AAA model of access control. The AAA model includes three major components. Authentication confirms that a user, device or service is who it claims to be, authorization ensures that users, devices and services may only perform actions that they are entitled to perform, accounting creates an audit trail of activity that maybe later verified.

Know the difference between identification and authentication. Access controls depend on effective identification and authentication. Subjects claim an identity and identification can be as simple as a username for a user. Subjects prove their identity by providing authentication credentials such as the matching password for a username. People, devices and services all verify their identity by giving proper credentials.

Understand the establishment of identity, registration and proofing. New employees establish their identities with official documentation such as a passport, driver's license or birth certificate. HR personnel then begin the registration process, which includes creating an account for a new employee. When biometric authentication is used, the registration process also collects biometric data. Identity proofing includes knowledge-based authentication and cognitive passwords. These ask users a series of questions that only the user would know the answers to.

Understand the difference between authorization and accounting. After authenticating subjects, systems authorized access to objects based on their proven identity. Auditing logs and audit trails record events including the identity of the subject that performed in action. The combination of effective identification, authentication and auditing provides accountability.

Know the primary authentication factors. The three primary factors of authentication are something you know such as a password or pin, something you have such as a smart card or authenticator device and something you are based on biometrics. Multifactor authentication MFA includes two or more authentication factors and using MFA is more secure than using a single authentication factor.

Understand important authentication concepts. Passwords are the weakest form of authentication, but password policies help increase their security by enforcing complexity and history requirements. Smart cards include microprocessors and cryptographic certificates and authenticators create one-time passwords. Biometric methods identify users based on characteristics such as fingerprints. The crossover error rate identifies the accuracy of a biometric method and shows where the false rejection rate is equal to the false acceptance rate. Lower crossover error rates are more accurate.

Understand single sign-on. Single sign-on or SSO is a mechanism that allows subjects to authenticate

once and access multiple objects without authenticating again. Describe how federated identity systems are implemented. Federated identity management systems are implemented on premises providing the most control via a third-party cloud service or as a hybrid of both. Describe just in time provisioning. Just in time or JIT provisioning creates user accounts on third-party sites the first time a user logs onto the site. JIT reduces the administrative workload.

Know about credential management systems. Credential management systems help developers easily store usernames and passwords and then retrieve them when a user revisits a website. The W3C published the credential management API as a working draft in 2019 and developers commonly use it as a credential management system. It allows users to log on automatically to websites without entering their credentials again.

Explain session management. Session management processes help prevent unauthorized access by closing unattended sessions. Developers commonly use web frameworks to implement session management. These frameworks allow developers to ensure sessions are closed after a specific amount of inactivity such as after two minutes.

Understand the identity and access provisioning lifecycle. The identity and access provisioning lifecycle refers to the creation, management and deletion of accounts. Provisioning ensures that accounts have appropriate privileges based on task requirements and employees receive any needed hardware. Onboarding processes inform employees of organizational processes. Deprovisioning processes disable or delete an account when employees leave and off-boarding processes ensure that employees return all the hardware and organization issued to them.

Explain the importance of group and role definition and transition. When an organization creates new job roles, it's important to identify privileges needed by anyone in these new roles. Doing so ensures that employees in these new roles do not have excessive privileges. These roles are commonly mapped to groups in the authentication system and then privileges are assigned to those roles. When users transition from one job to another, their group membership should be modified to follow those changes.

Describe the purpose of account access reviews. Account access reviews are performed on user accounts including privileged accounts, system accounts and service accounts. These reviews ensure that accounts don't have excessive privileges. They can often detect when accounts have excessive privileges and when unused accounts have not been disabled or deleted. Those are the study essentials that you need to know for Chapter 13, managing identity and authentication.