Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 16 of the official CISSP study guide. Here are the top things you need to know from this chapter on managing security operations. Know the difference between need to know and least privileged. Need to know and the least privileged principle are two standard IT security principles implemented in secure networks. They limit access to data and systems so that users and other subjects can access only what they require. This limited access helps prevent security incidents and helps limit the scope of incidents when they occur. When these principles are not followed, security incidents result in far greater damage to the organization.

Understand segregation of duties and job rotation. Segregation of duties is a basic security principle that ensures that no single person can control all critical functions or system elements. With job rotation, employees are rotated into different jobs or tasks are assigned to different employees. Collusion is an agreement among multiple persons to perform some unauthorized or illegal actions. Implementing these policies helps prevent fraud by limiting actions individuals can do without colluding with others.

Know about monitoring privileged operations. Privileged entities are trusted, but they can abuse their privileges, because of this, it's essential to monitor all assignment of privileges and the use of privileged operations. The goal is to ensure that trusted employees do not abuse the special privileges that they are granted. Monitoring these operations can also detect many attacks, because attackers commonly use special privileges during an attack. Advanced privileged account management practices can limit the time that users have advanced privileges.

Understand service level agreements. Organizations use service level agreements, SLAs with outside entities such as vendors. These agreements stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations. Describe personnel safety and security concerns. Duress systems allow guards to raise alarms in response to emergencies and emergency management plans help the organization respond to disasters. When employees travel, they need to be aware of the risks, especially if they travel to different countries. Safety training and awareness programs ensure that employees know about these risks and ways to mitigate them.

Understand secure provisioning concepts. Secure provisioning of resources includes ensuring that resources are deployed in a secure manner and are maintained in a secure manner throughout their life cycles. Asset management tracks tangible assets, hardware and software and intangible assets such as patents, trademarks, the company's goodwill and copyrights.

Know how to manage and protect media. Media management techniques track media used to hold sensitive data. Media is protected throughout it's lifetime and destroyed when it is no longer needed. Know the difference between SaaS, PaaS and IaaS. Software as a service SaaS models provide fully functional applications typically accessible by a web browser. Platform as a service PaaS models provide consumers with a computing platform including hardware, operating systems and a runtime environment. Infrastructure as a service IaaS models provide basic computing resources such as servers, storage and networking.

Know about serverless architecture. Serverless architecture is a cloud computing concept where code is managed by the customer and the platform i.e. supporting hardware and software or server is managed by the cloud service provider. There is always a physical server running the code, but this execution model allows a software designer to focus on the logic of their code and not to be concerned about the parameters or limitations of a specific server. This is also known as function as a service. Recognized security issues with managed services in the cloud. Managed services in the cloud include any resources stored in or accessed by the cloud. Storing data in the cloud increases

the risks, so additional steps maybe necessary to protect data depending upon it's value.

When leasing cloud-based services, you must understand who is responsible for maintenance and security. The cloud service provider provides the least amount of maintenance and security in the IaaS model. Explain configuration and change control management. Many outages and incidents can be prevented with effective configuration and change management programs. Configuration management ensures that systems are configured similarly and the configuration of systems are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point and imaging is a common baselining method. Change management helps reduce outages or weaken security from unauthorized changes. A change management process requires that changes be requested, reviewed, approved, tested, scheduled, implemented and documented. Versioning uses a labeling or numbering system to track changes and updated versions of software.

Understand patch management. Patch management ensures that systems are kept up to date with current patches. You should know that an effective patch management program will evaluate, test, approve and deploy patches. Additionally, be aware that system audits verify the deployment of approved patches to systems. Patch management is often intertwined with change and configuration management to ensure that documentation reflects the changes. When an organization does not have an effective patch management program, it will often experience outages and incidents from known issues that could have been prevented.

Explain vulnerability management. Vulnerability management includes routine vulnerability scans and periodic vulnerability assessments. Vulnerability scanners can detect known security vulnerabilities and weaknesses such as the absence of patches or weak passwords. They generate reports that indicate the technical vulnerabilities of a system and are an effective check for a patch management program. Vulnerability assessments extend beyond just technical scans and can include reviews and audits to detect vulnerabilities. Those are the study essentials that you'll need to know for Chapter 16, managing security operations.