**Chapter 16: Managing Security Operations**

The need-to-know principle imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks.

The least privilege principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more. Keep in mind that privilege in this context includes both permissions to data and rights to perform systems tasks.

Separation of duties (SoD) and responsibilities ensures that no single person has total control over a critical function or system. This is necessary to ensure that no single person can compromise the system or its security. Instead, two or more people must conspire or collude against the organization, which increases the risk for these people.

Two-person control (sometimes called the two-man rule) requires the approval of two individuals for critical tasks.

Job rotation (sometimes called rotation of duties) means that employees rotate through jobs or rotate job responsibilities with other employees. Using job rotation as a security control provides peer review, reduces fraud, and enables cross-training. Cross-training helps make an environment less dependent on any single individual.

Many organizations require employees to take mandatory vacations in one-week or two-week increments. This provides a form of peer review and helps detect fraud and collusion.

Privileged account management (PAM) solutions restrict access to privileged accounts or detect when accounts use any elevated privileges.

A service level agreement (SLA) is an agreement between an organization and an outside entity, such as a vendor. The SLA stipulates performance expectations and often includes penalties if the vendor doesn’t meet these expectations.

Duress (During Stress) systems are useful when personnel are working alone. A simple duress system is just a button that sends a distress call. A monitoring entity receives the distress call and responds based on established procedures.

Scalability refers to the ability of a system to handle additional workloads by adding additional resources.

Elasticity refers to a system’s ability to add and remove resources dynamically, based on

increasing or decreasing load.

Configuration management (CM) helps ensure that systems are deployed in a secure, consistent state and that they stay in a secure, consistent state throughout their lifetime. Baselines and images are commonly used to deploy systems.

A change management process ensures that personnel can perform a security impact analysis. Experts evaluate changes to identify any security impacts before personnel deploy the changes in a production environment.

Versioning typically refers to version control used in software configuration management. A labeling or numbering system differentiates between different software sets and configurations.

Configuration documentation identifies the current configuration of systems. It identifies who is responsible for the system and its purpose and lists all changes applied to the baseline.

A patch is a blanket term for any type of code written to correct a bug or vulnerability or to improve existing software performance. The software can be either an operating system or an application. Patches are sometimes referred to as updates, quick fixes, and hot fixes.

Vulnerability management refers to regularly identifying vulnerabilities, evaluating them, and taking steps to mitigate risks associated with them.

Vulnerability scanners are software tools used to test systems and networks for known security issues. A vulnerability scan enumerates (or lists) all the vulnerabilities in a system.

Vulnerabilities are commonly referred to using the Common Vulnerability and Exposures (CVE) dictionary. The CVE dictionary provides a standard convention used to identify and describe vulnerabilities. MITRE maintains the CVE database.