Summary This chapter addressed the data lifecycle within the cloud environment as well as specific security challenges in each phase. We reviewed the data lifecycle in the cloud as well as different data storage architectures that might be implemented in the cloud, the types of threats that those storage types and designs can face, and ways to protect storage. We reviewed encryption, including the importance of and difficulties with key and certificate management. We explored why we might want to obfuscate data and only display selected portions during operations, and you learned about various methods for performing this task. Next, we reviewed logging, log analysis, and SIEM solutions as well as how and why they’re implemented and some risks associated with their use. Finally, we addressed the topic of egress monitoring, how DLP tools work, and specific problems that might be encountered when trying to deploy DLP solutions in the cloud.

Exam Essentials Understand the risks and security controls associated with each phase of the cloud data life cycle. Explain what the risks to data are in each phase and which controls you would select to address the risks. **Understand the various cloud data storage architectures.** Be able to differentiate between long- term, ephemeral, and raw storage as well as file- based storage, block storage, and databases. **Understand how and why encryption is implemented in the cloud.** Understand the role of cryptography and encryption in securing cloud data. Know the essential elements of key management, why keys must be kept securely, and the risks of key compromise or exposure. Apply key management and certificate management technologies like hardware security modules, key escrow, and certificate revocation lists. **Be familiar with the practice of obscuring data.** Know the different techniques of data masking, hiding, anonymization, and tokenization. Explain hashing and its role in data obfuscation. **Be familiar with logging, storage, and analysis of data events and the use of SIEM technology.** Understand the purposes of SIEM implementation and the challenges associated with using those solutions. Explain the challenges and importance of logging in cloud environments. Describe key data elements like identities, IP addresses, and geolocation for event data. **Understand the importance of egress monitoring.** Be familiar with the goals of data loss prevention solutions; how they are implemented; how data is identified using tags, pattern matching, and labels; and what challenges a cloud customer might face trying to implement DLP within the cloud.