Summary In this chapter, we've discussed the core concepts required to design and build a secure data center. That process includes deciding whether to build a data center or to lease space in a preexisting data center. It also includes deciding where it should be located as well as ensuring redundancy and resilience are part of the design. Along the way we explored power, communications, and utility resilience as well as physical security design elements. You learned about data center tiers ranging from Tier 1 self- hosting facilities to Tier 4 highly available environments. Logical design is also a critical part of data center design. Understanding how access control and tenant partitioning help to ensure that shared facilities are secure for each tenant is necessary to manage a secure data center. Virtualization operations, including hypervisor management and security, resource scheduling, optimization, maintenance, and high availability are all part of modern data centers. Clustering and ensuring storage resilience is another element that data center operators and customers need to pay attention to. Finally, security operations, including security operations centers, that provide continuous monitoring and management of data center environments are needed. Tools like firewalls, security groups, IDS and IPS systems, honeypots, and a wide range of other technologies are combined to build a secure data center environment. With tools in place, organizations need to focus on incident management and incident response capabilities for when something goes wrong. **Exam Essentials Design and describe a secure data center.** Understand the buy versus build decision for data centers. Describe physical design considerations including location, utilities redundancy, and facilities redundancy elements. Explain environmental design components related to HVAC, multivendor pathways, and other redundant components necessary to data center operations. Outline the logical design elements of tenant partitioning and access controls. **Understand how redundancy is implemented in the design of the cloud data center.** Explain how each critical infrastructure element can be implemented in a redundant and resilient way, including utilities like power, water, and connectivity; processing capabilities; and data storage. Consider how emergency services and business continuity capabilities can be built into data center design. **Ensure the availability of clustered hosts and guest operating systems.** Describe methods of ensuring high availability for virtualized systems. Understand technologies like containerization and serverless functionality and how they relate to virtualization and cloud environments. Explain distributed resource scheduling and dynamic optimization and how they differ. Know when to use maintenance mode and what it means in a virtualization cluster. Understand storage clusters and their impact on availability and resilience. Explain data dispersion for data resilience. **Describe access controls for both local and remote access methods.** Explain the most common remote access methods for systems in a data center, including RDP, SSH, and virtual clients. Describe jump boxes and bastion hosts. Understand the role and application of secure terminals and console- based security mechanisms for physical access. **Explain network security controls as part of a cloud environment.** Explain common network security controls including firewalls and network security groups, IDSs/IPSs, honeypots, and bastion hosts. Describe the role of a SOC and how incident response occurs in a cloud data center environment.