1. List and briefly define the fundamental security design principles.

2. Describe the risk analysis approach and the steps in a detailed or formal risk analysis.

3. Describe the basic principles utilized in mandatory access control. How do these basic principles help MAC control the dissemination of information?

4. What is a message authentication code?

5. What is the security of a virtualization solution dependent upon? What are some recommendations to address these dependencies?

6. List the items that should be included in an IT security implementation plan.

7. Describe the inference problem in databases. What are some techniques to overcome the problem of inference?

8. Explain why input validation mitigates the risks of SQL injection attacks.

9. What are the benefits and risks of server-side scripting?

10. What is the difference between persistent and non-persistent cross-site scripting attacks?

11. What is the main purpose of DNS? Give three different techniques that an attacker can use to make a victim send DNS requests to domains chosen by the attacker.

12. Why are pharming and phishing attacks often used in concert with each other?

13. Describe the integrity levels introduced in Windows Server 2008. What features did these integrity checks allow Windows to implement?

14. Define three types of intellectual property.

15. Give an example of a computer crime. What are some unique issues associated with such crimes?

16. List and briefly describe three cloud service models.

17. What are the disadvantages to database encryption?

18. What are three broad mechanisms that malware can use to propagate?

19. What are the typical phases of operation for a virus or worm?