Assignment 1

Q1. Alyssa is responsible for her organization's security awareness program. She is concerned that changes in technology may make the content outdated. What control can she put in place to protect against this risk?

A. Gamification
B. Computer-based training
C. Content reviews
D. Live training

Q2. Gavin is creating a report for management on the results of his most recent risk assessment. In his report, he would like to identify the remaining level of risk to the organization after adopting security controls. What term best describes this current level of risk?

A. Inherent risk
B. Residual risk
C. Control risk
D. Mitigated risk

Q3. Lisa is attempting to prevent her network from being targeted by IP spoofing attacks as well as preventing her network from being the source of those attacks. Which of the following rules are best practices that Lisa should configure at her network border? (Select all that apply.)

A. Block packets with internal source addresses from entering the network.
B. Block packets with external source addresses from leaving the network.
C. Block packets with public IP addresses from entering the network.
D. Block packets with private IP addresses from exiting the network.

Q4. Ed has been tasked with identifying a service that will provide a low-latency, high-performance, and high-availability way to host content for his employer. What type of solution should he seek out to ensure that his employer's customers around the world can access their content quickly, easily, and reliably?

A. A hot site
B. A CDN
C. Redundant servers
D. A P2P CDN

Q5. Fran is building a forensic analysis workstation and is selecting a forensic disk controller to include in the setup. Which of the following are functions of a forensic disk controller? (Select all that apply.)

A. Preventing the modification of data on a storage device
B. Returning data requested from the device
C. Reporting errors sent by the device to the forensic host
D. Blocking read commands sent to the device