MGT 442 - Information Security Risk Management
Practice Questions

Practice Test

Please complete the following questions without using your book. After completing the test, we will review the answers as a class.

1. Which of the following would **NOT** be included in an exception request? Circle the correct answer:

   A. How the risk was discovered
   B. How you plan to address the risk
   C. Who will be responsible for addressing the risk
   D. Any compensating controls that you think already meet the intention or lessen the risk
   E. A graph of the identified risks
   F. The affected environment or user community

2. Which of the following is considered a vulnerability? Circle the correct answer:

   A. Learning or guessing user account passwords
   B. Unauthorized use of services and assets
   C. Poor key management
   D. Unauthorized disclosure or modification of information
   E. Denial of service attack

3. Which of the following is NOT considered an accountability control? Circle the correct answer:

   A. Disk Encryption
   B. Monitoring and Alerting
   C. Supervision
   D. Logging (physical and logical)
   E. Individual Accounts
   F. Digital Signatures

4. Match the following controls with their primary function. Each category should only be used once:

_____ Recovery Plan

_____ Application Proxy

_____ Header Masking

_____ Access Control Lists

Mitigation Categories:

A. Can reduce the threat universe
B. Can negate the vulnerability
C. Can increase difficulty of exploit
D. Can limit the effects of the exploit

5. Match the following risks/threats with their threat category. Categories can be used more than once and not every category must be used:

_____ Disgruntled employee

_____ Trojan horse, virus, malicious application is received from SPAM mail

_____ Payroll error due to employee information data entry mistake

_____ Power failure due to electrical storms

_____ Corporate espionage

Threat Categories:

A. Infrastructure Failure
B. Accidents
C. External Targeted Attack
D. Internal Abuse
E. External Mass Attack
F. Natural Disaster

6. Match the following controls with their control category. Categories can be used more than once and not every category must be used:

_____ Network Intrusion Monitoring

_____ Penetration Testing & Remediation

_____ Procedures to Restore Data from Archive

_____ Security Awareness Training

Control Categories:

A. Risk Alleviation

B. Risk Limitation

C. Risk Planning

7. Put the following phases of the NIST Risk Management workflow in order. Mark the first step in the process with a "1", and the last with a "6":

_____ Assess Controls

_____ Select Controls

_____ Authorize System

_____ Monitor Controls

_____ Categorize System

_____ Implement Controls

8. Calculate the Annual Loss Exposure (ALE) given the following details:

- Each laptop in your company costs $1,000 to replace
- Based on your asset tracking records, you have estimated 1 laptop gets stolen every 2 years
- There is no other value associated with these laptops

Based on this scenario, what is the ALE for this risk? Circle the correct answer:

A. $200

B. $500

C. $1,000

D. $2,000

E. $365,000

9. Match the following terms with their definitions:

_____ Qualitative Risk Rating

_____ Quantitative Risk Rating

A. An absolute measure of risk exposure based on historical statistics and numeric evaluations of risk factors

B. A relative measure of risk exposure based on approximations or generalizations of risk factors

10. True or False, according to the FAIR framework, the terms “frequency” and “probability” are equivalent and can be used interchangeably in risk assessments? Circle the correct answer:

A. True

B. False