---

**Table of Contents**



# 1. Exam - Introduction

**Survivability Is an enterprise-wide concern**

Overview: These are the exam questions for Principle 1: Survivability Is an Enterprise-Wide Concern.

Answer the following questions based on this scenario:

*You are the IT manager at XYZ Corporation. Your staff is responsible for maintaining the corporate network infrastructure (routers, switches, external network connectivity, etc.). You have started an initiative to increase survivability of the IT infrastructure. Your boss, the CIO, says "I thought we had a firewall and intrusion detection system. Why do we need any other security stuff?"*



**1.1.** How would you describe the difference between survivability and security to the CIO?

**Security is the defense of the CIA traits of information and systems where the end goal is simply that defense of the information, while survivability focuses on the ability of information to be available and protected within the context of the mission of the organization. Security is a component of survivability, but survivability is more focused on mission accomplishment.**

**1.2.** The CIO says that security is an overhead expense that he cannot afford. Therefore, your initiative for survivability will effectively go nowhere since there will be no funding for it. What would you tell the CIO about the costs of survivability verses security?

**The costs of security are often considered overhead expenses. Survivability, however, has the end goal of successful mission accomplishment, and therefore is seen as an investment in the organization that brings tangible returns. The costs of survivability are all**

**operationally sound since they involve the operations organizations of the enterprise and require input from those business units.**

**1.3.** What does the "layered approach" to survivability mean?

**Survivability defenses should be applied in layers such that they provide redundancy and fault tolerance to the enterprise.**

**1.4.** Give a non-IT example of a layered approach to survivability and describe the layers and how they work together.

**United States Postal Service, Military base.**

**Multiple Choices:** Circle the best choice(s) to answer each of the following questions according to the information given in Principles:

1.1. Which of the following groups should be concerned with system survivability?
1.2. Which of the following are characteristics of traditional computer security?
1.3. A fundamental assumption to the concept of survivability is that
1.4. Compared with "bounded" network systems, "unbounded" network systems have
1.5. Which of the following are key properties for a survivable system to maintain its capability to deliver essential services?
1.6. Which of the following are example items of information asset?
1.7. Employment of user access controls in a network system belongs to what type of information asset protection strategy?
1.8. Which of the following are threats or risks to critical information assets?
1.9. Which of the following are examples of system vulnerabilities?
1.10. Which of following are possible means that can be exploited by intruders?

**1.1.** Which of the following groups should be concerned with system survivability?

a. Security experts
b. Top level management
c. Risk management staff
d. System Administrators
e. End users

**1.2.** Which of the following are characteristics of traditional computer security?

a. Focus on continuity of operations
b. Systems are under central administrative control
c. Consider security cost an overhead expense
d. View security as part of enterprise risk management
e. Protect system components as the primary mission

**1.3.** A fundamental assumption to the concept of survivability is that

a. Technology based solutions are necessary for handling attacks, accidents, or failures.
b. Secured systems are always capable of surviving attacks, accidents, or failures.
c. No system is totally immune to attacks, accidents, or failures.
d. Firewall is the best way to help a system survive attacks, accidents, or failures.

**1.4.** Compared with "bounded" network systems, "unbounded" network systems have

a. more central organizational control
b. less visibility to systems and users
c. clear distinction between system insiders and outsiders
d. well-defined geographic, legal, and technological boundaries
e. more shared and uncertain tasks for system administrators

**1.5.** Which of the following are key properties for a survivable system to maintain its capability to deliver essential services?

a. Recover of essential services in the wake of an attack
b. Detect and evaluate attacks and intrusions
c. Repel and resist attacks
d. Prevent any future attacks from happening

**1.6.** Which of the following are example items of information asset?

a. Hard copy documents
b. Banking transactions stored on tapes
c. Customer addresses stored on a network drive
d. Flat panel LCD monitor
e. Wireless email traveling in the air

**1.7.** Employment of user access controls in a network system belongs to what type of information asset protection strategy?

a. Avoidance
b. Prevention
c. Detection
d. Recovery

**1.8.** Which of the following are threats or risks to critical information assets?

a. Disclosure of the information
b. Transmission of the information
c. Modification of the information
d. Theft or interruption of the information
e. Encryption of the information

**1.9.** Which of the following are examples of system vulnerabilities?

a. Viruses and worms
b. Buffer overflows
c. Denial of service
d. Lack of documentation
e. Network sniffing

**1.10.** Which of following are possible means that can be exploited by intruders?

a. Software tools
b. Internet chat rooms
c. Mailing lists
d. System information
e. Social engineering

**Fill in Blanks:** Fill in the blank(s) in each of the following statements with key words using the information given in Principle 1.

1. Survivability refers to the capability of a system to _____, _____, in the presence of attacks, failures, and accidents.
2. In the light of survivability, systems are seen as _____, _____, with _____ administrative control.
3. Unbounded network systems with connections to the Internet are subject to increased _____ that impact their survivability.
4. The capability of a system to maintain essential properties, such as specified levels of _____, _____, _____, and other quality attributes, is critical to the delivery of essential services.
5. Information assets categories include _____, _____, _____, and _____.
6. A comprehensive approach to implementing and sustaining information security can include these strategies and practices: _____, _____, _____, _____, _____, _____.
7. Vulnerability is defined as _____ of a safeguard.
8. Crackers are individuals who attempt to _____.
9. Hackers are individuals who are more interested in probing systems and networks for their own _____ rather than actually causing harm.
10. Script kiddies are _____ who use sophisticated tools available to break into computer systems although they lack the knowledge to craft the tools themselves.

**Suggested answers:**

**Multiple Choice:**

1. a, b, c, d, e
2. b, c, e
3. c

4. b, e
5. a, b, c
6. a, b, c, e
7. b
8. a, c, d
9. b, d
10. a, b, c, d, e

**Fill in blanks:**

1. fulfill its mission, in a timely manner
2. open, unbounded, distributed
3. threats and attacks/intrusions
4. integrity, confidentiality, performance
5. information, hardware, software, people
6. avoidance, prevention, detection, containment and response, recovery, improvement
7. the absence or weakness
8. maliciously alter systems for their benefit
9. enjoyment and curiosity
10. intruders