CONCORDIA COLLEGE
MOORHEAD, MINNESOTA

- Name: _____
- Date: _____
- Section: _____

BUSN 315: Management Information Systems

Quiz #4: Suggested Solutions

Spring 2026

INSTRUCTIONS:

- Write your name, date, and section clearly at the top of the first page.
- This is a closed-book quiz. Do not use your textbook, class notes, or electronic devices.
- The quiz consists of three parts: True / False, Multiple Choice, and Short Answers.
- For multiple-choice questions, circle the single best answer. Only one option is correct.
- For short-answer questions, write your responses in complete sentences. Limit each response to at most five sentences.
- You have 75 minutes to complete the quiz. Manage your time carefully.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Problem 1. True / False **(5 Points Each)**

Determine whether each statement is TRUE or FALSE. If FALSE, justify briefly.

1.A. VPNs eliminate the need for authentication systems.

- FALSE
  VPNs encrypt communication channels but do not verify user identity on their own. Authentication systems are still required to ensure that only authorized users can access the network.

1.B. Bandwidth refers to the maximum capacity of a connection to transmit data.

- TRUE

1.C. Delaying patches can increase the risk of a security breach.

- TRUE

1.D. A Trojan horse appears legitimate but contains hidden malicious functions.

- TRUE

Problem 2. True / False **(4 Points Each)**

Determine whether each statement is `TRUE` or `FALSE`. If `FALSE`, justify briefly.

2.A. The Domain Name System (DNS) translates IP addresses into human-readable domain names.

- `FALSE`
  DNS translates human-readable domain names (e.g., google.com) into IP addresses, not the other way around.

2.B. Search Engine Marketing (SEM) involves the use of paid advertisements to increase visibility in search results.

- `TRUE`

2.C. Information systems security refers only to technologies such as firewalls and encryption, not organizational policies.

- `FALSE`
  Information systems security includes not only technologies, but also organizational policies, procedures, and user practices.

2.D. Multifactor authentication (MFA) relies on a single type of credential for verification.

- `FALSE`
  MFA requires multiple types of credentials (e.g., password + verification code), not just one.

Problem 3. Multiple Choice **(3 Points Each)**

Select the BEST answer for each question based on course concepts discussed in class.

3.A. Which of the following best describes a digital network?

a) A centralized database used for storing business records
b) A collection of connected devices that can communicate and exchange data
c) A system used only for Internet browsing
d) A set of software tools for web design

3.B. Which of the following best explains why networks matter for managers?

a) Networks eliminate the need for business strategy
b) Networks lower costs and expand organizational reach
c) Networks remove all security risks from communication
d) Networks ensure that all firms use the same software

3.C. Which of the following best describes the role of a router?

a) It connects different networks together
b) It manages user permissions on a network
c) It stores files for multiple clients
d) It creates web pages using HTML

3.D. Which of the following best describes the Internet?

a) A private network used only by businesses
b) A single large server that stores all websites
c) A global network connecting millions of private and public networks
d) A system used only for email communication

Problem 3. Multiple Choice (continued) **(3 Points Each)**

Select the BEST answer for each question based on course concepts discussed in class.

3.E. TCP/IP is important because it:

a) defines how data is packaged, addressed, transmitted, and received

b) creates web pages using hyperlinks

c) encrypts all network traffic automatically

d) replaces the need for IP addresses

3.F. A company wants employees in remote locations to stay connected through the same data infrastructure used for ordinary Internet communication. Which concept best fits this situation?

a) Wireless broadband

b) Search engine optimization

c) Data mining

d) Digital forensics

3.G. Which of the following best describes Voice over Internet Protocol (VoIP)?

a) A technology that converts voice signals into digital packets that travel across IP networks

b) A system that uses separate phone networks for local calls

c) A protocol that creates websites for businesses

d) A tool used to optimize search rankings

3.H. A firm adopts a cloud-based platform that combines voice, video, messaging, and email in one place. This is best described as:

a) Unified Communications as a Service (UCaaS)

b) Search Engine Marketing (SEM)

c) A Network Interface Controller (NIC)

d) A transmission medium

Problem 3. Multiple Choice (continued) **(3 Points Each)**

Select the BEST answer for each question based on course concepts discussed in class.

3.I. A company wants remote employees to safely access internal corporate systems across the Internet using encrypted connections. Which technology best fits this need?

a) DNS

b) VPN

c) RSS

d) HTML

3.J. Which of the following best distinguishes SEO from SEM?

a) SEO uses paid ads, while SEM improves organic visibility

b) SEO improves organic visibility, while SEM uses paid search ads

c) SEO is used for email communication, while SEM is used for websites

d) SEO and SEM are identical concepts

3.K. Which of the following best describes security in information systems?

a) Policies, procedures, and technologies used to prevent unauthorized access, alteration, or damage

b) Protecting only hardware from physical damage

c) Systems used to increase Internet speed

d) Software used to design web pages

3.L. Which of the following best describes the goal of security policies?

a) To eliminate all system vulnerabilities

b) To guide how an organization protects its information assets

c) To increase network speed

d) To reduce hardware costs

Problem 4. Short Answers #1 **(7 Points Each)**

A mid-sized company is evaluating ways to modernize its communication systems. Currently, it uses a traditional telephone system that operates separately from its data network. The IT manager proposes switching to a system where voice calls are transmitted over the same Internet connection used for email, file sharing, and video conferencing. Some employees express concerns about call quality and mention that the company recently upgraded its office Wi-Fi network to improve Internet speed. Others point out that the company has multiple office locations and frequently makes long-distance and international calls.

4.A. What technology is the IT manager proposing?

- Voice over Internet Protocol (VoIP).

4.B. Explain one key advantage of this technology compared to the company's traditional telephone system. In your answer, focus on how this technology changes the way communication is handled.

- Cost reduction: Uses Internet infrastructure, reducing costs for long-distance and international calls.
- Integration of communication tools: Combines voice, video, messaging, and email into a single platform.
- Scalability and flexibility: Easier to add users or expand across multiple office locations without new hardware.
- Support for remote work: Employees can make and receive calls from anywhere with Internet access.
- Simplified infrastructure: Eliminates the need to maintain separate voice and data networks.
- Mobility: Users are not tied to a physical phone line and can use multiple devices.

Problem 5. Short Answers #2 **(7 Points Each)**

A financial services company is notified by a software vendor about a known vulnerability in one of its core systems. The vendor provides a patch to fix the issue. However, the company delays installing the update because management is concerned about potential system downtime during business hours. At the same time, the company has recently implemented stricter password policies and employee cybersecurity training programs. Several weeks later, attackers exploit the vulnerability and gain unauthorized access to sensitive customer information.

5.A. What security management issue is illustrated in this scenario?

- Failure to apply timely security patches (poor patch management).

5.B. Explain why delaying the installation of updates can increase the risk of a security breach.

- Exposure to known vulnerabilities: Attackers can exploit publicly known weaknesses that have not yet been patched.
- Availability of exploit tools: Once vulnerabilities are disclosed, attack tools are often developed and shared.
- Longer attack window: Delays increase the time during which systems remain vulnerable.
- False sense of security: Other measures do not fix underlying software flaws.
- Targeting by attackers: Organizations that delay updates may be specifically targeted as easier victims.
- Compounding risk over time: Multiple unpatched vulnerabilities increase overall system risk.

- Original Score: _____
- Original Date: _____
- Recovered Score: _____
- Recovered Date: _____