WESTERN GOVERNORS UNIVERSITY (WGU) HUMN1101 D333 ETHICS IN TECHNOLOGY PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-humn1101-d333.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What does reliability in a system primarily refer to?

A. Efficiency of resource use

B. Ability to function effectively over time

C. Speed of processing information

D. Cost of maintenance and repair

2. Cyberterrorism is intended to intimidate which group(s)?

A. Only government officials

B. Civilians and government populations

C. Corporate executives

D. Educational institutions

3. What is an example of a behavior that would be considered a vice?

A. Altruism

B. Honesty

C. Greed

D. Integrity

4. What is system testing primarily concerned with?

A. Testing individual subsystems separately.

B. Evaluating the complete system as a unified entity.

C. Performing data entry procedures.

D. Conducting user experience surveys.

5. What is the purpose of a next-generation firewall (NGFW)?

A. To enhance user privacy

B. To block basic internet threats

C. To detect and block sophisticated attacks

D. To encrypt network data

6. What factor is vital to achieving supply chain sustainability?

A. Using the cheapest materials available.

B. Ensuring energy efficiency and minimizing waste.

C. Focusing exclusively on local suppliers.

D. Prioritizing technological advancements over environmental concerns.

7. What does green computing emphasize?

A. Maximizing profit through IT

B. Efficient use and disposal of IT products

C. Enhancing software performance

D. Reducing IT support costs

8. Which of the following best defines electronically stored information (ESI)?

A. Information stored in physical files

B. Any digital information in various formats

C. Only emails and social media posts

D. Encrypted databases only

9. Which of the following best describes cyberterrorism?

A. Cyberattacks for educational purposes

B. Digital threats without intent to cause harm

C. Utilization of IT to disable infrastructure for political gain

D. Friendly hacking to improve security

10. What term describes the legal standard that defendants with expertise are evaluated against?

A. Competency standard

B. Negligence standard

C. Redundancy

D. Expertise standard

Answers

1. B
2. B
3. C
4. B
5. C
6. B
7. B
8. B
9. C
10. C

Explanations

1. What does reliability in a system primarily refer to?

A. Efficiency of resource use

B. Ability to function effectively over time

C. Speed of processing information

D. Cost of maintenance and repair

Reliability in a system primarily refers to its ability to function effectively over time. This concept emphasizes how consistently and dependably a system performs its intended functions without failure. A reliable system is one that can be counted on to operate correctly and efficiently under specified conditions throughout its lifespan, minimizing downtime and the risk of malfunctions. This aspect of reliability is crucial in technology and engineering, as it affects user trust and satisfaction. Users expect systems to work as intended, and any inconsistency or failure can lead to significant operational disruptions. Therefore, a system's reliability not only enhances performance but also contributes to overall productivity and efficiency in various applications. While aspects like efficiency of resource use, speed of processing, and maintenance costs are important in evaluating a system's performance, they do not capture the essence of reliability, which is fundamentally about consistent performance over time.

2. Cyberterrorism is intended to intimidate which group(s)?

A. Only government officials

B. Civilians and government populations

C. Corporate executives

D. Educational institutions

Cyberterrorism is designed to instill fear and panic in a broad audience, which typically includes both civilians and government populations. This form of terrorism leverages technology to create disruptions that can affect national security, economic stability, and public safety. By targeting systems critical to society, such as infrastructure, communication networks, or financial systems, cyberterrorists aim to send a message that can cause cognitive deterrence and social unrest. The rationale is that by implicating a wide range of individuals, the impact is magnified, creating fear that extends beyond specific groups. Thus, civilians, as members of the general public, alongside government entities that are responsible for maintaining order and security, are both seen as essential targets. This comprehensive targeting distinguishes it from other forms of intimidation that focus on narrower groups such as corporate executives or educational institutions, which, while they can be targeted in specific attacks, do not encompass the broader societal goal inherent in cyberterrorism.

3. What is an example of a behavior that would be considered a vice?

A. Altruism

B. Honesty

C. Greed

D. Integrity

Greed is considered a vice because it represents an excessive desire for wealth or possessions, often at the expense of ethical considerations or the well-being of others. This behavior reflects a self-centered mindset, prioritizing personal gain over collective good and disregarding the impact on others. Vices are typically associated with negative traits or actions that lead to harm or unethical behavior. In contrast, the other options—altruism, honesty, and integrity—are all qualities that reflect positive moral character and ethical behavior, promoting the welfare of others and a sense of trustworthiness. Thus, greed stands out as a behavior indicative of moral failings, making it a clear example of a vice.

4. What is system testing primarily concerned with?

A. Testing individual subsystems separately.

B. Evaluating the complete system as a unified entity.

C. Performing data entry procedures.

D. Conducting user experience surveys.

System testing is primarily concerned with evaluating the complete system as a unified entity. This phase of testing aims to ensure that the integrated components of the software work together as intended, highlighting the collective behavior of the application. It verifies that all functional and non-functional requirements are met when the system operates as a whole, addressing interactions between subsystems and ensuring overall system stability and performance. By focusing on the complete system, testers can identify issues that may not be apparent when examining individual units or subsystems in isolation. This collaborative evaluation is critical for understanding how the different parts of the system interact and for ensuring that the final product is robust and capable of handling real-world scenarios. In contrast, testing individual subsystems separately would fall under unit testing or integration testing rather than system testing, while performing data entry procedures and conducting user experience surveys are more related to usability testing and validation of workflows within the application.

5. What is the purpose of a next-generation firewall (NGFW)?

A. To enhance user privacy

B. To block basic internet threats

C. To detect and block sophisticated attacks

D. To encrypt network data

The purpose of a next-generation firewall (NGFW) is primarily to detect and block sophisticated attacks. Unlike traditional firewalls that mainly focus on monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, NGFWs integrate advanced capabilities such as deep packet inspection, intrusion prevention systems (IPS), and application awareness. This allows them to identify complex threats that could bypass less advanced security measures. Next-generation firewalls can analyze traffic at a much deeper level, considering factors like the applications being used, user identity, and the context of the data. This capability enables them to defend against emerging threats that exploit sophisticated techniques, such as advanced persistent threats (APTs) and zero-day exploits. By blocking these sophisticated attacks, NGFWs play a crucial role in maintaining the security of networks in a landscape filled with evolving cyber threats. While enhancing user privacy, blocking basic internet threats, and encrypting network data are important aspects of cybersecurity, they do not encapsulate the primary function of NGFWs as comprehensively as the detection and blocking of sophisticated attacks.

6. What factor is vital to achieving supply chain sustainability?

A. Using the cheapest materials available.

B. Ensuring energy efficiency and minimizing waste.

C. Focusing exclusively on local suppliers.

D. Prioritizing technological advancements over environmental concerns.

Ensuring energy efficiency and minimizing waste is a fundamental factor in achieving supply chain sustainability. This focus not only reduces the environmental impact of productions and services but also leads to cost savings in the long run. By adopting practices that enhance energy efficiency, organizations can reduce their carbon footprint, utilize resources more effectively, and contribute to a healthier planet. Additionally, minimizing waste reflects a commitment to sustainable practices, encouraging recycling and the responsible disposal of materials. This holistic approach promotes long-term viability and ethical responsibility within the supply chain, aligning business practices with environmental stewardship.

7. What does green computing emphasize?

A. Maximizing profit through IT

B. Efficient use and disposal of IT products

C. Enhancing software performance

D. Reducing IT support costs

Green computing emphasizes the efficient use and disposal of IT products, which involves practices focused on minimizing environmental impact and promoting sustainability. This includes designing energy-efficient hardware, using sustainable materials, and implementing measures for recycling and proper disposal of electronic waste. The goal of green computing is to reduce the ecological footprint of technology, ensuring that IT practices contribute positively to environmental preservation. This approach not only seeks to lower energy consumption and reduce harmful waste but also promotes a responsible and ethical framework for technology use in a way that is mindful of future generations. The other options revolve around profit maximization, software performance enhancement, and cost reduction, which are important business considerations but do not align with the core principles of green computing focused on sustainability and responsible environmental stewardship.

8. Which of the following best defines electronically stored information (ESI)?

A. Information stored in physical files

B. Any digital information in various formats

C. Only emails and social media posts

D. Encrypted databases only

The definition of electronically stored information (ESI) encompasses a wide range of digital information found in various formats. This includes documents, emails, databases, presentations, spreadsheets, and more, regardless of the specific medium or format used to store the data. The broad nature of this definition reflects the diverse array of ways information can be captured and preserved in digital environments, making it crucial in legal and business contexts where data retrieval and analysis may be required. While some options mention specific types of storage or types of information, they do not accurately cover the comprehensive scope of what constitutes ESI. The all-encompassing nature of "any digital information in various formats" effectively captures the essence of ESI and its significance in the realm of technology and information management.

9. Which of the following best describes cyberterrorism?

A. Cyberattacks for educational purposes

B. Digital threats without intent to cause harm

C. Utilization of IT to disable infrastructure for political gain

D. Friendly hacking to improve security

The choice that accurately describes cyberterrorism is the utilization of IT to disable infrastructure for political gain. This definition encapsulates the essence of cyberterrorism, which involves the use of technology to carry out attacks that can disrupt critical infrastructure, leading to significant harm or potentially instilling fear within a society. Such actions are often politically motivated and intended to coerce or intimidate governments or populations. Cyberterrorism goes beyond just digital attacks; it specifically aims at achieving political objectives through means that leverage information technology, targeting systems essential for functioning, such as power grids, transportation systems, and communication networks. This can result in significant societal disruption and can have dire consequences for public safety and national security. In contrast, other options depict scenarios that do not reflect the nature of cyberterrorism. Activities framed as educational or friendly hacking are usually focused on enhancing security or learning, without harmful intentions, which is not aligned with the malicious and disruptive goals of cyberterrorism. Additionally, digital threats lacking intent to cause harm do not fall under the category of cyberterrorism, as the key component of intent to instill fear or achieve political aims is missing.

10. What term describes the legal standard that defendants with expertise are evaluated against?

A. Competency standard

B. Negligence standard

C. Redundancy

D. Expertise standard

The legal standard that is applied to defendants with expertise is typically referred to as the "competency standard." This standard evaluates whether the defendant acted within the bounds of what is considered reasonable and acceptable for someone with their level of expertise. For example, professionals such as doctors, engineers, or other experts are expected to demonstrate a certain level of knowledge and skill that aligns with their profession. If their actions fall below this accepted standard, they may be found negligent. In this context, the competency standard serves as a benchmark for assessing the performance of individuals in specialized fields. It helps determine if a defendant's actions were appropriate given their professional background and the circumstances surrounding their case. Thus, the concept of evaluating based on established professional standards highlights the expectations placed on individuals who possess specialized knowledge and skills.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://wgu-humn1101-d333.examzify.com

We wish you the very best on your exam journey. You've got this!