



Global Knowledge™

Expert Reference Series of White Papers

7 Types of Hard CISSP Exam Questions and How To Approach Them

7 Types of Hard CISSP Exam Questions and How To Approach Them

Doug Landoll, General Manager, Security Services, En Pointe, CISSP, CISA



Introduction

The first thing most people hear about the CISSP examination is how difficult or unfair the questions are. Although this may be a good warning, it does not begin to prepare you to do well on the exam itself. For some of the CISSP exam questions, just knowing the facts is not enough. These questions are referred to as “hard questions”. This paper examines seven types of hard questions you are likely to see on the CISSP examination and the best approaches for solving them.

Throughout the CISSP preparation course offered by Global Knowledge, we cover the various security mechanisms, principles, concepts, and facts that will be included on the CISSP exam. A large portion of the CISSP examination will test your knowledge of these aspects. However, the mere knowledge of these aspects does not prepare you for the more difficult questions you may see on the CISSP examination. This is why the Global Knowledge CISSP preparation class is not limited to a review of the information security mechanisms, principles, concepts, and facts. A significant portion of the course is devoted to study skills, memorization techniques, application of concepts, and principles. Although it is impossible to predict exactly what questions you may get on the exam, we have classified the difficult questions into seven categories and given examples and approaches for identifying and overcoming them.

1.1 Detailed Knowledge Questions

Description

Requires a detailed knowledge of a technology or principle.

Example Question

At what level of the OSI model can a packet be corrected on the bit level?

- a) Level 2
- b) Level 3
- c) Level 4
- d) Level 5

Answer

The correct answer is a) Level 2. Level 2 is the data link level. More specifically, Media Access Control is a sub level of Level 2 that performs error control. If a single bit is in error, it can either flag it as an error or, in the case of parity bits, it can rebuild the frame and perform a bit-level error correction. Also note that Level 4 (transport) also performs error control, but it is based on a packet. If an error is detected at Level 4 it can only request a re-transmission. This is just a hard question. You may know the OSI stack very well and still miss this question.

Approach

Study well, and think the question through. Even though the CISSP is commonly described as “a mile wide and an inch deep”, you still have to know the security-relevant aspects of mechanisms and techniques. Take several approaches at comparing and contrasting similar and alternative mechanisms. For example, error correction can be done at Level 2, Level 4, and even Level 7. Ask yourself, “What is the difference between error correction at Levels 2, 4, and 7?” At the same time make sure you understand the difference between the four output modes of DES. For example, why would someone use ECB over CBC?

1.2 Subset Questions

Description

These are questions where at least two of the answers are right but one is *more right* than the others. As it turns out, we find that many of these types of questions can be viewed as a subset question in which one or more of the answers are actually subsets of the most correct answer.

Example Question

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

- a) Spoofing attack
- b) Surveillance attack
- c) Social engineering attack
- d) Man-in-the-middle attack

Answer

The correct answer is c) Social engineering attack. Both a) and c) involve misleading, but only social engineering involves contact with the user (social) and leads toward a bad security decision (engineering).

Approach

First you need to recognize this as a subset question. Draw arrows from one answer to another if you believe that the first answer is a subset of the second. Then ask yourself if the “inner” answer is always correct or not. If the subset answer is always correct, then pick that one. If not, pick the one that is correct

1.3 Too Much Information Questions

Description

This is a type of question that gives you too much information. The candidate is sometimes fooled into finding an appropriate equation to use all of the variables offered in the question.

Example Question

When performing a risk assessment you have developed the following values for a specific threat/risk pair. Asset value = 100K, exposure factor = 35%; Annual rate of occurrence is 5 times per year; the cost of a recommended safeguard is \$5000 per year, which will reduce the annual loss expectancy in half. What is the SLE?

- a) \$175,000
- b) \$35,000
- c) \$82,500
- d) \$77,500

Answer

The correct answer is b) \$35,000. SLE is simply AV x EF. a) is ALE; c) the ALE improvement given the safeguard is put in place; d) is the safeguard value.

Approach

Having formulas memorized is only half the battle. Recognizing the question from the word problem is the other half. It is not difficult to find the question. But when we feel rushed, it is easy to overlook the question and simply move forward and create an equation to fit the available data. The questions are ready for you and have bogus answers that will match your calculations.

1.4 Application Questions

Description

These questions are applied knowledge questions. You may very well understand the concepts, definitions, and technical details of a security mechanism. But that is not enough. You must also be able to apply this knowledge. These questions can be difficult because it may be hard to determine the specific principle the question is testing you on.

Example Question

The primary entry to a secured area has implemented a proximity card reader for entry into the main entry during working hours and a PIN code required in addition to the proximity card for access to the main entry after hours. What type of access control is most appropriate for the secondary entry?

- a) Proximity card / PIN code
- b) Cipher lock
- c) Motion-sensor activated entry lock
- d) Deadbolt latch on inside

Answer

The correct answer is d) Deadbolt latch on inside. This application question tests your ability to reason and your knowledge about secondary entry/exits. The best security posture has a single entry to secured areas. But if a secondary exit is required for fire/safety reasons, people need to be able to exit through the door. However, that door should not be used as an entry. A panic bar is another reasonable implementation and might appear as an option. Answers a), b), and c) all assume that the secondary exit should be accessible from the outside—which it should not.

Approach

First, narrow the question down by removing the clearly incorrect answers. In the example above b) Cipher lock and c) Motion sensor activated entry lock both provide less protection than a two-factor control like a) Proximity card / PIN code.

Second, determine the difference between the remaining answers. Choice a) Proximity card / PIN code assumes the same protection on the secondary entry. On the other hand, choice d) assumes no entry, only an exit for emergencies. The principle being tested here is the fact that you only want a single entry point into a secure area.

1.5 Technical Definition Questions

Description

These questions are rather straightforward and simply ask you to define a technical information security term. However, because of the multiple sources for “standard” definitions, you may not be familiar with the description given.

Example Question

The task that includes the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment is called:

- a) Risk evaluation
- b) Penetration testing
- c) Threat analysis
- d) Vulnerability assessment

Answer

The correct answer is c) Threat analysis. The definition is a direct quote from a National Institute of Standards Special Publication (NIST SP800-27) entitled Generally Accepted Engineering Principles. Answers a), b), and d) all rely on threat identification as a component of the task but each of these goes farther to find vulnerabilities, penetrate systems, or even compute risks and recommend safeguards.

1.6 Poorly Worded Questions

Description

These questions are simply worded poorly. They come about either because the test question writer has difficulty expressing ideas in words (possible) or believes that this type of question more accurately separates those who know the material from those who don't (more likely). Regardless, there is an easy way to tackle this type of question.

Example Questions with Interpretations:

Type	Example	Interpretation
Double negative	Which of the following are not disadvantages of	Advantage
Words for numbers	On average one third of the asset is protected from exposure completely eliminating the threat.	EF = 66.67% ALE after = \$0
Unfamiliar terms or phrases	Which of the following would increase the risk of the security posture? reduces the assurance of A clipping level is used to	Something bad Something bad Threshold

Approach

Use a variety of techniques to ensure the words don't throw you off. For example:

1) Keyword Highlighting. Recognize the key phrase or word and underline it. This technique will train you to read the questions more carefully.

2) Plus / Minus Approach. Translate the underlined portion of the question into a more simply worded question. For example, reduce the question to a "good" or "plus" vs. "bad" or "minus" question. In this case, mark your examination booklet near the question with a plus or minus sign. Then, when reviewing the candidate answers for that question, mark each of those with a plus or minus. Don't worry if it is a weak or strong mechanism; simply mark it as positive or negative. Eliminate any candidate answer that does not match the question's sign. This approach will focus your thinking on the validity of each candidate answer and away from the clumsy wording of the question.

1.7 Graphically-Challenged Questions

Description

The CISSP examination test booklet is text only. There are no graphics or tables in the exam booklet. Some questions, however, could benefit from the insertion of a related graphic to more clearly illustrate the questions.

Example Question

The addressing mode in which an instruction references a memory location that contains the address of the data value is referred to as:

- a) Immediate addressing
- b) Direct addressing
- c) Indirect addressing
- d) Relative addressing

Answer

The correct answer is c) indirect addressing. Indirect addressing is the addressing mode in which a pointer to the address that contains the data is contained within the instruction.

Approach

However, this set of words does little to clarify the concept. The picture below assists greatly with the understanding of this concept.

If a graphic helps to explain the concept, then a graphic generated from the text of the question will help you to answer the question. Bottom line: If you wish the question had a graphic – create one.

Conclusion

Although you still have many facts to memorize before you take the exam, you now should have a better understanding of the types of questions you might face. If a question on the exam appears difficult at first, don't fret. Simply take a moment to identify its type, and apply the methods listed here to work your way through it.

Good luck!

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course:

[CISSP Prep Course](#)

For more information or to register, visit www.globalknowledge.com or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Douglas Landoll has 18 years' information security experience. Mr. Landoll has led security risk assessments establishing security programs within top corporations and government agencies. He is an expert in security risk assessment, security risk management, security criteria, and building corporate security programs.

His background includes evaluating security at the NSA, NATO, CIA, and other government agencies; co-founding the Arca Common Criteria Testing Laboratory, co-authoring the SSE-CMM, teaching at NSA's National Cryptologic School; and running the southwest security services division for Exodus Communications. Presently, Mr. Landoll is the President of Veridyn. Mr. Landoll is a CISSP and CISA. He holds a CS degree from James Madison University and an MBA from the University of Texas at Austin. Mr. Landoll has published numerous information security articles, speaks regularly at conferences, and serves as an advisor for several high-tech companies. Mr. Landoll is the author of the recently published *The Security Risk Assessment Handbook*.