CISM® QAE ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

PURPOSE OF THE CISM QAE ITEM DEVELOPMENT GUIDE

The purpose of the CISM Item Development Guide (Guide) is to provide assistance to item writers in their efforts to develop items for the *CISM® Review Questions, Answers & Explanations* (QAE) *Manual.* This Guide explains the structure of CISM QAE questions and will assist item writers in becoming more skilled in writing items.

As you read through the Guide, please pay particular attention to the item writing principles. Applying these principles will greatly enhance the chances of your items being accepted.

PURPOSE OF THE CISM QAE

The purpose of the *CISM® Review Questions, Answers & Explanations Manual (QAE)* is to provide the CISM candidate with similar questions and testing topics to help prepare and study for the CISM exam. The questions in this publication are not actual CISM exam questions, but are intended to provide CISM candidates with an understanding of the type and structure of questions that typically appear on the exam.

CISM EXAM STRUCTURE

ISACA and the CISM Certification Committee periodically perform a CISM Job Practice Analysis study to determine the tasks and knowledge currently required of information security managers. The results of this analysis serve as the blueprint for the CISM exam. Questions must be written to test a candidate's knowledge of established process and content areas defined by the CISM Job Practice Analysis.

WRITING QUALITY ITEMS

The first thing to consider when writing an item is its target audience, or the CISM candidate. An item must be developed at the proper level of experience (three-to-five years of information security management work experience) expected of a successful CISM candidate.

While writing items, one must take into consideration that information security management is a global profession and individual perceptions and experiences might not reflect the more global position or circumstance. Because the exam and CISM items are developed for the international information security community, this will require the item writer to be somewhat flexible when determining a globally accepted practice.

Note that items submitted for consideration by the CISM QAT must be original items created by the item writer. Items previously submitted for consideration by any TES for any exam or any QAT cannot be submitted to the CISM QAT and vice versa.

MULTIPLE-CHOICE ITEMS

The CISM exam consists of multiple-choice items. The multiple-choice item is the most commonly used type of test question in certification exams.

Multiple-choice items consist of a stem and four possible options.

Item Stem:
The item stem is the introductory statement or question that describes a situation or circumstance related to the knowledge being assessed. Item stems can be written in the form of an incomplete statement as well as in question form.

Item Options:
The options complete the introductory statement or answer the question and consist of one correct answer (key) and three incorrect answers or distracters.

Key:
The key must reflect current practice. In some cases the key will be the only correct choice, while in other cases the key will be deemed to be the BEST choice when considered with the other choices provided.

Distracters:
Distracters are the incorrect options but should be plausible or possible correct answers to candidates who are not knowledgeable enough to choose the key.

STEPS TO WRITING ITEMS

STEP 1 Select a topic within the CISM Job Practice. Items should be written to test knowledge necessary to perform a specific task. Items should focus on a single topic or knowledge statement. Items written from a knowledge statement will most likely result in higher quality, practice-based questions. Refer to Appendix A "CISM Job Practice" for a list of the task and related knowledge statements.

Once a topic is chosen, follow the steps listed below. While writing your item, please refer to the Item Writing Principles for further guidance and review your item using the Item Development Checklist found in Appendix B.

STEP 2 Write the item stem and keyable answer (Answer A).

STEP 3 Develop plausible distracters. The distracters should not be made up words or phrases. Distracters should appear to be correct choices to an inexperienced professional. The development of quality distracters is usually the most difficult task for an item writer. If you have difficulty with this part of item development, consult with your colleagues. Also think about what an inexperienced IT professional might think the correct answer would be. These incorrect experiences make for the best distracters.

STEP 4 Include a thorough justification of why the keyable answer is correct as well as why each distracter is not a correct choice. It is not acceptable to simply state that the distracters are incorrect.

STEP 5 Include any and all reference sources. Refer to the ISACA web site for applicable references – http://www.isaca.org/knowledge-center.

STEP 6 Review the item using the Item Development Checklist found in Appendix B.

STEP 7 Have a peer or colleague review and critique the item.

GENERAL ITEM WRITING PRINCIPLES

DOs:

1. Write the stem in the positive tone. Negatively written items will be automatically returned to the item writer for rewrite.
2. Test only one testing concept or knowledge statement per item. Knowledge statements were developed for this purpose. For a listing of knowledge statements, refer to Appendix A, "CISM Job Practice."
3. Ensure that the stem and all options are compatible with each other. For example, if your stem reads, "Which of the following controls will BEST…," then all options must be controls.
4. Keep the stem and options as short as possible by avoiding the use of unnecessary text or jargon. Do not attempt to teach the candidate a concept or theory by providing too much information before asking the question.
5. Include common words or phrases in the item stem rather than in the key and distracters.
6. Write all options the same approximate length and format. A good test taker with very little knowledge or experience in IT will select the option that is either the shortest or the longest in length and will most likely choose the correct answer.
7. Write options that are grammatically consistent with the item stem and maintain a parallel grammatical format. For example if the key begins with a verb ending with "ing," then all distracters must begin with a verb ending with "ing."
8. Use only professionally acceptable or technical terminology in the item stem and options

DON'Ts:

1. Avoid using a key word or phrase in the item key that appears in the stem. Experienced test takers will look for clues such as this that often identify the key.
2. The use of words such as "frequently," "often," "common" or "rarely" introduce subjectivity into the item and will not be accepted. If an item is subjective, it can be argued that more than one option is keyable. Subjectivity is the most common reason why items are returned to the item writer and not tested on exams.
3. The use of terms in the stem such as "always," "never" or "all" are not acceptable since very little is absolute and thus it makes it easier for candidates to eliminate distracters.
4. Terms such as "least," "not," or "except" are negative and require a candidate to choose an incorrect or least preferred choice, rather than a correct or preferred choice. Negatively phrased test questions do not test well and will not be accepted.
5. Avoid the use of gender pronouns such as he, she, his or her.
6. Avoid multiple components within each option, or including portions of one option in another. These are considered to be "multiple, multiple choice options" and do not test well. Each option should stand on its own.
7. Items with options "all of the above" or "none of the above" will be returned to the item writer. Good test takers know that these types of options are very rarely correct and do not make good distracters.

8. Items testing knowledge regarding vendor specific products will be returned to the item writer as ISACA does not endorse any vendor products.
9. Items will not be accepted if they list specific standards, frameworks, manuals (i.e., COBIT, ISO) by name. It is, however, perfectly acceptable and encouraged to test the knowledge associated with these best practices.
10. Avoid testing subjective concepts such as the following:
    a. Specific international or local laws and regulations.
    b. Specific information regarding cultural or industry issues that do not apply globally and across all industries.
    c. Specific roles and responsibilities within your organization.

Remember that the CISM exam is administered globally and across all industries and the concepts tested must be accepted and recognized practice globally and in all industries.

ITEM EXAMPLES

Items can either be direct questions, incomplete statements or scenario descriptions. Below are examples of these three types of questions. These questions were developed as sample items for item writing training and do not appear on any exam.

Direct question:

Stem: Which of the following will **BEST** tie information security to business objectives?

Options:
A. Value analysis
B. Security metrics
C. Deliverables list
D. Process improvement model

Note that the stem is in the form of a question.

Incomplete statement:

Stem: The **PRIMARY** goal of a post-incident review is to:

Options:
A. identify ways to improve the response process.
B. gather evidence for subsequent legal action.
C. identify individuals who failed to take appropriate action.
D. make a determination as to the identity of the attacker.

Note that the responses for this item are followed by a period, as the response serves to complete the sentence started in the stem.

SCENARIO QUESTIONS

There are a number of considerations when writing scenario questions.
This type of item consists of introductory information (or the scenario) for the items to follow.

- There should be a set of two-to-five items that pertain to this introductory information.
- The introductory material must be related to a particular field, be relevant, practical and contain all the information necessary for the candidate to draw the correct conclusion – do not force the candidate to make assumptions.
- The associated items should be in some sort of sequence and follow a logical progression.
- Each item should be independent of the other items so that missing one item does not cause missing another item of the set. Care should be taken to ensure that one item does not point to the key of another item.
- New information cannot be introduced in any of the associated items. All information necessary to answer the question must be in the scenario or introductory information.

The best scenarios are written on real-life situations faced on the job. Also, the more subjective concepts such as regulations and roles and responsibilities are good to test within a scenario as you can explain the specifics requirements of the regulation or the organization's reporting structure in the introductory paragraph(s).

WHAT TO AVOID WHEN CONSTRUCTING ITEMS

Following are items to illustrate what to avoid when constructing quality items. Again, these questions are not CISM pool questions and will not appear on any exam. They were developed as sample items for item writing training purposes.

Example 1:

Stem: An intrusion prevention system does which of the following?

Options:
A. Prevents any attacks that occur from affecting the target system
B. Stops all network traffic that is part of an attack before that traffic can get to the intended victim
C. Constantly modifies operating systems to make them a moving target
D. Launches attacks against attacking systems to bring them down or disable them

Key: A

Notice that a key word from the stem "prevent" is in the answer. Avoid using important words in the stem and the answer or any of the distracters. Also, absolute words are used in options B (all) and C (constantly) making them easily eliminated. Avoid using absolute or subjective terms in the options.

Example 2:

Stem: Which of the following is **MOST** important to writing good information security policies?

Options:
A. Ensure that they are easy to read and understand
B. Ensure that they allow for flexible interpretation
C. Ensure that they describe technical vulnerability
D. Ensure that they change whenever operating systems are upgraded

Key: A

Notice that the first three words are repeated in each item. This question can be easily rewritten to make it a more concise item. Simply include the three words at the end of the stem.

New Stem: Which of the following is **MOST** important to writing good information security policies? Ensure that they:

Options:
A. are easy to read and understand.
B. allow for flexible interpretation.
C. describe technical vulnerability.
D. change whenever operating systems are upgraded.

The stem becomes an incomplete sentence with the options completing the sentence.

Example 3:

Stem: When building support for an information security program, which of the following should be performed **FIRST**?

Options:
A. Identification of existing vulnerabilities
B. Cost-benefit analysis
C. Business impact analysis
D. Formal risk assessment

Key: A

Note: This is an example of a timing question and introduces subjectivity. Both options C and D could be the correct answer depending on the situation within a given organization.

Testing what is to be done FIRST does not test well unless there is a definite FIRST step in a process. However, when there is a definite FIRST step, then the question becomes too easy.

Example 4:

Stem: Security awareness programs should be:

Options:
A. standardized throughout the organization.
B. customized depending on the target audiences.
C. avoided since key security vulnerabilities may be disclosed.
D. limited to IS personnel.

Key: A

Note: This is another example of a subjective item. In some organizations, security awareness programs are mandated to be standardized and in others, they prefer programs to be customized. The answer depends on the organization's security needs and program.

When writing questions on areas that tend to be subjective in nature, such as what makes for a good information security awareness program, or testing roles and responsibilities, be very careful to ensure that there is only one correct answer in all situations. If you cannot ensure this, then add more content to the stem or write a scenario question to take away the subjectivity. For example, you could describe an organization's structure so that it is clear to an experienced information security manager what type of security awareness program would perform best.

Example 5:

Stem: Record retention policies generally are driven by:

Options:
A. risk levels acceptable to the organization.
B. legal and regulatory requirements.
C. business goals and objectives.
D. audit and assurance requirements.

Key: A

This question illustrates the effect of having weak distracters or too obvious of an answer. Answers like legal/regulatory requirements make for poor questions because there are no other strong options to distract candidates away from the correct choice.

The previous examples represent the most common reasons why items are not accepted. Another reason an item may not be accepted is because it is too technical. Remember, when writing items for the CISM exam, the content needs to test the knowledge of an experienced information security MANAGER, not a technician. Also remember that the CISM exam is a practical examination testing an individual's application of information security management knowledge. Another common reason why items are returned is because they are definitional in nature. This means that the item is simply asking the candidate whether they know the definition of a technology or terminology; not how to apply it.

CISM JOB PRACTICE – WHAT IS IT?

The CISM Job Practice lists the relevant tasks performed by IT professionals working in the area of information security and the knowledge necessary to perform those tasks. These tasks and knowledge will be the basis for CISM exam questions. The goal of the CISM exam is to write practice-based questions testing knowledge necessary to perform a task. The CISM Job Practice can be found in Appendix A. Remember, it is important to focus on only one knowledge statement or testing concept when writing questions.

RUBRICING

All items must be assigned a rubric. The rubric indicates which CISM task and knowledge statement the item most closely refers to. Each rubric consists of a 2 to 3-digit task statement number AND a 2 to 3-digit knowledge statement number. The rubrics are indicated before each task and knowledge statement. Please refer to Appendix A—CISM JOB PRACTICE when rubricing an item.

ITEM SUBMISSION AND REVIEW PROCESS

All subject matter experts that have indicated an interest in CISM item writing will receive periodic emails (item writing campaigns). Item writing campaigns will also include deadlines as to when items are to be submitted for review.

Items must be submitted to CISMQAE@isaca.org. All items MUST be submitted in English using the form located in Appendix C – Item Construction Form. All fields within the Item Construction Form must be complete. If fields are left blank, your item will be returned without review.

An initial review will be performed by an ISACA representative to ensure completeness and compliance with the item writing principles. Items that are judged to be flawed in any significant way will be sent back to the item writer with appropriate and constructive feedback. Items accepted by the ISACA representative will be forwarded to the CISM Quality Assurance Team (QAT) to be considered for inclusion in the *CISM® Review Questions, Answers & Explanations* (QAE) *Manual.*

Once reviewed by the CISM QAT, the item will be accepted or returned. If returned, the item will be sent back to the item writer and will also include appropriate and constructive feedback. If accepted, the item will become the property of ISACA and the item writer will receive honorarium payment. ISACA awards an honorarium of US $100 for items accepted by the QAT along with 2 CPE credit hours.

Items submitted for consideration by the CISM QAT must be original items created by the item writer. Items previously submitted for consideration by any TES for any exam or any QAT cannot be submitted to the CISM QAT and vice versa.

Appendix A

CISM Job Practice

Domain 1 – Information Security Governance: Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately, and program resources are managed responsibly.

Task Statements:

1.1 Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
1.2 Establish and maintain an information security governance framework to guide activities that support the information security strategy.
1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
1.4 Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures, and guidelines.
1.5 Develop business cases to support investments in information security.
1.6 Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.
1.7 Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
1.8 Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
1.9 Establish, monitor, evaluate, and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

Knowledge Statements:

KS1.1 Knowledge of methods to develop an information security strategy
KS1.2 Knowledge of the relationship among information security and business goals, objectives, functions, processes, and practices
KS1.3 Knowledge of methods to implement an information security governance framework
KS1.4 Knowledge of the fundamental concepts of governance and how they relate to information security
KS1.5 Knowledge of methods to integrate information security governance into corporate governance
KS1.6 Knowledge of internationally recognized standards, frameworks and best practices related to information security governance and strategy development
KS1.7 Knowledge of methods to develop information security policies
KS1.8 Knowledge of methods to develop business cases
KS1.9 Knowledge of strategic budgetary planning and reporting methods
KS1.10 Knowledge of the internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) and how they impact the information security strategy

KS1.11 Knowledge of methods to obtain commitment from senior management and support from other stakeholders for information security
KS1.12 Knowledge of information security management roles and responsibilities
KS1.13 Knowledge of organizational structure and lines of authority
KS1.14 Knowledge of methods to establish new, or utilize existing, reporting, and communication channels throughout an organization
KS1.15 Knowledge of methods to select, implement, and interpret metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])

Domain 2 – Information Risk Management and Compliance: Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.

Task Statements:

2.1 Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
2.2 Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
2.3 Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted periodically and consistently to identify risk to the organization's information.
2.4 Determine appropriate risk treatment options to manage risk to acceptable levels.
2.5 Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
2.6 Identify the gap between current and desired risk levels to manage risk to an acceptable level.
2.7 Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
2.8 Monitor existing risk to ensure that changes are identified and managed appropriately.
2.9 Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.

Knowledge Statements:

KS2.1 Knowledge of methods to establish an information asset classification model consistent with business objectives
KS2.2 Knowledge of methods used to assign the responsibilities for and ownership of information assets and risk
KS2.3 Knowledge of methods to evaluate the impact of adverse events on the business
KS2.4 Knowledge information asset valuation methodologies
KS2.5 Knowledge of legal, regulatory, organizational and other requirements related to information security
KS2.6 Knowledge of reputable, reliable, and timely sources of information regarding emerging information security threats and vulnerabilities
KS2.7 Knowledge of events that may require risk reassessments and changes to information security program elements
KS2.8 Knowledge of information threats, vulnerabilities, and exposures and their evolving nature
KS2.9 Knowledge of risk assessment and analysis methodologies
KS2.10 Knowledge of methods used to prioritize risks
KS2.11 Knowledge risk reporting requirements (for example, frequency, audience, components)
KS2.12 Knowledge of methods used to monitor risks
KS2.13 Knowledge of risk treatment strategies and methods to apply them
KS2.14 Knowledge of control baseline modeling and its relationship to risk-based assessments
KS2.15 Knowledge of information security controls and countermeasures and the methods to analyze their effectiveness and efficiency
KS2.16 Knowledge of gap analysis techniques as related to information security
KS2.17 Knowledge of techniques for integrating risk management into business and IT processes
KS2.18 Knowledge of cost/benefit analysis to assess risk treatment options

Domain 3- Information Security Program Development and Management: Establish and manage the information security program in alignment with the information security strategy.

Task Statements:

3.1 Establish and maintain the information security program in alignment with the information security strategy.
3.2 Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement, and IT) to support integration with business processes.
3.3 Identify, acquire, manage and define requirements for internal and external resources to execute the information security program.
3.4 Establish and maintain information security architectures (people, process, technology) to execute the information security program.
3.5 Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
3.6 Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
3.7 Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline.
3.8 Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline.
3.9 Establish, monitor, and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Knowledge Statements:

KS3.1 Knowledge of methods to align information security program requirements with those of other business functions
KS3.2 Knowledge of methods to identify, acquire, manage, and define requirements for internal and external resources
KS3.3 Knowledge of information security technologies, emerging trends (for example, cloud computing, mobile computing), and underlying concepts
KS3.4 Knowledge of methods to design information security controls
KS3.5 Knowledge of information security architectures (for example, people, processes, technology) and methods to apply them
KS3.6 Knowledge of methods to develop information security standards, procedures, and guidelines
KS3.7 Knowledge of methods to implement and communicate information security policies, standards, procedures, and guidelines
KS3.8 Knowledge of methods to establish and maintain effective information security awareness and training programs
KS3.9 Knowledge of methods to integrate information security requirements into organizational processes
KS3.10 Knowledge of methods to incorporate information security requirements into contracts and third-party management processes

KS3.11 Knowledge of methods to design, implement, and report operational information security metrics

KS3.12 Knowledge of methods for testing the effectiveness and applicability of information security controls

Domain 4 – Information Security Incident Management: Plan, establish, and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

Task Statements:

4.1 Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents.
4.2 Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
4.3 Develop and implement processes to ensure the timely identification of information security incidents.
4.4 Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
4.5 Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.
4.6 Organize, train, and equip teams to effectively respond to information security incidents in a timely manner.
4.7 Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.
4.8 Establish and maintain communication plans and processes to manage communication with internal and external entities.
4.9 Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness, and take appropriate remedial actions.
4.10 Establish and maintain integration among the incident response plan, disaster recovery plan, and business continuity plan.

Knowledge Statements:

KS4.1 Knowledge of the components of an incident response plan
KS4.2 Knowledge of incident management concepts and practices
KS4.3 Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan
KS4.4 Knowledge of incident classification methods
KS4.5 Knowledge of damage containment methods
KS4.6 Knowledge of notification and escalation processes
KS4.7 Knowledge of the roles and responsibilities in identifying and managing information security incidents
KS4.8 Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams.
KS4.9 Knowledge of forensic requirements and capabilities for collecting, preserving, and presenting evidence (for example, admissibility, quality and completeness of evidence).
KS4.10 Knowledge of internal and external incident reporting requirements and procedures
KS4.11 Knowledge of post-incident review practices and investigative methods to identify root causes and determine corrective actions
KS4.12 Knowledge of techniques to quantify damages, costs, and other business impacts arising from information security incidents

KS4.13 Knowledge of technologies and processes that detect, log, and analyze information security events

KS4.14 Knowledge of internal and external resources available to investigate information security incidents

Appendix B

Item Development Checklist

Before submitting an item, you must be able to answer YES to all of the following questions.

1. Does the item test a CISM concept at the appropriate experience level of the test candidate?

2. Does the item test only one CISM concept?

3. Is the item clear, concise and free of unnecessary or ambiguous terms?

4. Is there enough information in the stem to allow for only one correct answer? A candidate must not be able to interpret a distracter as correct based on assumptions due to a lack of information in the stem.

5. Is there only one possible or best answer in any situation, organization or culture? Many items are returned because there is more than one possible key based on situations not addressed in the stem.

6. Are the stem and all options compatible with each other? For example: “Which of the following controls…?” All options must be controls.

7. Does the item have plausible distracters but only one correct answer?

8. Does the item avoid words or phrases in the key that already appear in the stem?

9. Does the item avoid subjective terms such as “frequently,” “often” or “common” in the stem and options?

10. Does the item avoid absolute terms such as “all,” “never” or “always” in the stem and options?

11. Does the item avoid such terms as “least,” “not,” “except”?

Appendix C

ITEM CONSTRUCTION FORM

Name:
ISACA ID:
Task Statement: *(Refer to CISM Job Practice) This is mandatory; any items submitted without a task statement will be returned*
Knowledge Statement: *(Refer to CISM Job Practice) This is mandatory; any items submitted without a knowledge statement will be returned*

Testing Concept: (One sentence describing what is being tested) *This is mandatory; any items submitted without a testing concept will be returned*

Stem:

Options:
A. (Always make A the correct answer)
B.
C.
D.

Key: A

Justification:
A. (Why is A the correct answer)
B. (Why is B incorrect)
C. (Why is C incorrect)
D. (Why is D incorrect)

Reference(s): Provide references to enable independent review. Include the publication title, publication year, author and page.

