CRISC® ITEM DEVELOPMENT GUIDE

Updated March 2017

ISACA®
Trust in, and value from, information systems

CRISC ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

CRISC ITEM DEVELOPMENT GUIDE

PURPOSE OF THE CRISC ITEM DEVELOPMENT GUIDE

The CRISC Item Development Guide (Guide) provides CRISC item writers with an understanding of the concepts, structure and criteria of exam questions (items) to increase the quality and acceptance rate of new items for the CRISC exam. The Guide will also provide item writing principles and assist item writers in becoming more skilled in writing items.

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

CRISC EXAM STRUCTURE

The purpose of developing the CRISC Job Practice is to identify the tasks performed and knowledge required by professionals who are responsible for risk identification, assessment, evaluation, response, and monitoring, as well as for the design, implementation, monitoring, and maintenance of IS controls. This job practice serves as the blueprint for the CRISC exam. Questions must be written to test a candidate's knowledge of this content as defined by the CRISC Job Practice (see Appendix A, "CRISC Job Practice").

WRITING QUALITY ITEMS

When writing an item one must consider the exam's target audience, or the minimally competent CRISC candidate. An item must be developed at the proper level of experience expected of the individual just passing the CRISC exam. To qualify for the CRISC certification after passing the CRISC exam, one must have at least three (3) years of cumulative work experience across a minimum of two (2) CRISC domains. Of the two required domains, one must be risk-related, either Domain 1 (IT Risk Identification) or Domain 2 (IT Risk Assessment).

While writing items, one must also consider that the CRISC exam will be administered globally and items need to reflect the international IT and business community. This consideration requires item writers to be flexible when testing a globally accepted practice.

CRISC TERMINOLOGY

Because foundational terms such as "risk," "vulnerability," and "threat" are commonly misused in the industry, consistent use of these terms should be used in exam questions and answers. To standardize test language, please keep in mind that:

- "Risk" refers to the likelihood (or frequency) and magnitude of loss that exists from a combination of assets, threats, and control conditions. As a derived value, the word "risk" should not be used in the plural form (i.e. "risks"). Consequently, when referring to conditions that represent some amount of risk, please use the

terms "risk factors" or "risk scenarios." Be careful not use the terms "risk," "threat," or "vulnerability" interchangeably.

- "Threat" refers to actions or actors that may act in a manner that can result in loss or harm.
- "Vulnerability" refers to control conditions that are deemed to be deficient relative to requirements or the threat levels being faced.
- "Risk owner" refers to the person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario. (Scope note: the risk owner may not be responsible for the implementation of risk treatment.)

MULTIPLE-CHOICE ITEMS

The CRISC exam consists of 150 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 question or introductory statement that describes a situation or circumstance related to the knowledge being assessed. Item stems can be written in the form of a question or as an incomplete statement. Item stems should always be written in the positive tense. All negatively written items using the terms NOT, EXCEPT, LEAST are not tested since they unfairly force a test taker to reverse their thinking pattern. Test takers should always look for the correct solution to a situation as opposed to an incorrect solution.

Item Options:
The options answer the question or complete the introductory statement and consist of one correct answer (key) and three incorrect answers or distractors. To be most effective, all item options should have similar sentence structure and length.

Key:
The key is the correct or best answer. In some cases, the key will be the only correct choice, while in other cases the key will be the BEST choice when considered against the other choices provided.

Distractors:
Distractors are the incorrect options. They should be sufficiently believable or likely to divert candidates who are not knowledgeable in the field of practice from choosing the correct answer.

CRISC ITEM DEVELOPMENT GUIDE

STEPS TO WRITING ITEMS

STEP 1 Select a topic within the CRISC 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, experienced-based questions. Refer to Appendix A "CRISC 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(s), please refer to the Item Writing Principles for further guidance. Review your item(s) using the Item Development Checklist found in Appendix B.

STEP 2 Write the item stem and answer, which is referred to as the "key." (For item writing purposes, option "A" is always written as the key).

STEP 3 Develop plausible distractors. The distractors should not be made up words or phrases. Distractors should appear to be correct choices to an inexperienced professional. The development of quality distractors 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 distractors.

STEP 4 Include a thorough explanation of why the key/answer is correct as well as why each distractor is not a correct choice. It is not acceptable to simply state that the distractors are incorrect.

STEP 5 Include any and all reference sources. The ISACA web site is an excellent resource for references. Many applicable references may be found at 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, "CRISC 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. Remember, this is an exam, not a classroom.
5. Include common words or phrases in the item stem rather than in the key and distractors.
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 distractors 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 distractors.
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 pronouns (i.e., "you") and gender pronouns such as he/she, his/her/him.
6. 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 distractors.
7. Avoid multiple components within each choice, or including portions of one choice in another. These are considered to be "multiple-multiple" choices and do not test well. Each choice should stand on its own.
8. Items testing knowledge regarding vendor specific products will be returned to the item writer as ISACA does not endorse any vendor products.
9. Avoid "True/False" type questions, such as "Which of the following is true?"
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 CRISC 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 or incomplete statements.

Direct question:

Stem: Which of the following concerns would BEST be addressed by the comparison of production application systems source code with an archive copy?

Options:

A. File maintenance errors
B. Unauthorized modifications
C. Software version currency
D. Documentation discrepancies

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

Incomplete statement:

Stem: The comparison of production application systems source code with an archive copy would BEST address:

Options:

A. file maintenance errors.
B. unauthorized modifications.
C. software version currency.
D. documentation discrepancies.

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

It is wise to draft an item first as a direct question, and then revise it to an incomplete sentence if this offers smoother, less repetitive wording.

WHAT TO AVOID WHEN WRITING ITEMS

Following are examples of what to avoid when constructing items. Please note that these items or any items in this Guide will not appear on future exams.

Example 1:

Stem: A manager in the loan department of a financial institution performs unauthorized changes to the interest rate of several loans in the financial system. Which type of control could BEST have prevented this fraud?

Options:

A. Functional access controls
B. Logging of changes to loan information
C. Senior management supervision
D. Change management controls

Key: A

This item would be returned to the item writer because the stem assumes functional responsibility. The CRISC test is global and it is difficult to define functional responsibilities between countries and organizations. In some organizations, the loan department manager may have access.

Example 2:
Stem: Which of the following would represent the GREATEST risk when discovered during user access testing for a mission critical server?

Options:
A. Access is not based on least privilege
B. Access to sensitive data tables was granted without approval forms
C. Access reviews are not performed by the data owner
D. Monitoring of access is not performed by the data owner

Key: A

This item would be returned to the item writer because all of the options are keyable or correct. It is subjective and difficult to determine which risk is the greatest. Items must have one clear answer in all situations.

Example 3:
Stem: When performing automated vulnerability and penetration testing, which of the following would present the MOST concern?

Options:
A. Performing the test during peak processing hours.
B. Enabling an intrusion detection system during the test.
C. Denying access while scanning the firewall.
D. Consuming a high amount of resources on the system that is running the tool.

Key: A

This item would be returned as option D directly relates to option A and could be keyable. Option C is not understandable.

Example 4:
Stem: An intrusion prevention system does which of the following?

Options:
A. Prevents 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

This item would be returned to the item writer or rewritten because the term “prevention” in the stem leads directly to the term “prevent” in the key, making choice A the obvious answer.

CRISC ITEM DEVELOPMENT GUIDE

CRISC JOB PRACTICE – WHAT IS IT?

The CRISC Job Practice lists the relevant tasks performed by IT professionals working in the areas of risk and control and the knowledge necessary to perform those tasks. These task and knowledge statements will be the basis for CRISC exam questions. The goal of the CRISC exam is to present experience-based questions testing knowledge necessary to perform a task. The CRISC 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 CRISC task and knowledge statement the item most closely refers to. Each rubric consists of a task statement number AND a knowledge statement number. The rubric numbers are indicated before each task and knowledge statement. Please refer to Appendix A—CRISC JOB PRACTICE when rubricing an item. ***In the online submission form, rubrics are referred to as "Classifications." Task statements are "Primary Classifications" and knowledge statements are "Secondary Classifications."***

ITEM SUBMISSION AND REVIEW PROCESS

Items must be submitted using ISACA's online item writing system. All items MUST be submitted in English. Items must include a stem, four alternatives, and rationales for each alternative.

All subject matter experts who have signed up to write items at www.isaca.org/itemwriting will receive periodic emails announcing item writing campaigns. These emails will also contain a link to the item writing system. Documents relating to the campaign such as the specific areas of need, this Guide, and the Job Practice will be available for your reference.

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 CISA Exam Item Development Working Group (EIDWG) to be considered for inclusion in the exam item pool.

Once reviewed by the EIDWG, the item will be accepted or returned. If returned by the EIDWG, the item will be returned to the writer, including appropriate and constructive feedback. If accepted, the item will become the property of ISACA and the item writer will receive honorarium payment along with 2 CPE credit hours. An honorarium of US $100.00 will be awarded for each item accepted within the areas of need. Items accepted outside of the areas of need will be awarded US $50.00.

Appendix A
CRISC JOB PRACTICE

CRISC Task Statements

Domain 1 – IT Risk Identification: Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

1.1.1 Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations.

1.1.2 Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis.

1.1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.

1.1.4 Identify key stakeholders for IT risk scenarios to help establish accountability.

1.1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprisewide risk profile.

1.1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.

1.1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

Domain 2 – IT Risk Assessment: Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

1.2.1 Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.

1.2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

1.2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.

1.2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.

1.2.5 Communicate the results of risk assessment to senior management and appropriate stakeholders to enable risk-based decision making.

1.2.6 Update the risk register with the results of the risk assessment.

Domain 3 – Risk Response and Mitigation: Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

1.3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.

1.3.2 Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).

1.3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.

1.3.4 Ensure that control ownership is assigned to establish clear lines of accountability.

1.3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.

1.3.6 Update the risk register to reflect changes in risk and management's risk response.

1.3.7 Validate that risk responses have been executed according to the risk action plans.

Domain 4 – Risk and Control Monitoring and Reporting: Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

1.4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.

1.4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.

1.4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.

1.4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.

1.4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.

1.4.6 Review the results of control assessments to determine the effectiveness of the control environment.

1.4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

CRISC ITEM DEVELOPMENT GUIDE

CRISC Knowledge Statements

Please note: The task numbers (T) listed in parentheses after each of the knowledge statements refer to those tasks the knowledge statements most likely map to. It is entirely possible, based on the context of a given item, for a knowledge statement to map to a different task statement found in the Job Practice.

KNOWLEDGE OF:

1. laws, regulations, standards and compliance requirements (T1.1.1, 1.1.2, 1.1.3, 1.1.7, 1.2.1, 1.2.3, 1.3.3, 1.4.1)
2. industry trends and emerging technologies (T1.1.1, 1.1.2, 1.1.3, 1.1.7, 1.2.1, 1.2.2)
3. enterprise systems architecture (e.g., platforms, networks, applications, databases and operating systems) (T1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.3.3)
4. business goals and objectives (T1.1.1, 1.1.3, 1.1.6, 1.1.7, 1.4.1, 1.4.4)
5. contractual requirements with customers and third-party service providers (T1.1.1, 1.1.2, 1.1.3, 1.2.5)
6. threats and vulnerabilities related to:
    - 6.1. business processes and initiatives (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.4.1, 1.4.4)
    - 6.2. third-party management (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.3. data management (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.4. hardware, software and appliances (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.5. the system development life cycle (SDLC) (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.6. project and program management (T1.1.1, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.7. business continuity and disaster recovery management (DRM) (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.8. management of IT operations (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4)
    - 6.9. emerging technologies (T1.1.2, 1.2.1, 1.2.2, 1.2.3)
7. methods to identify risk (T1.1.1, 1.1.2, 1.1.3, 1.1.5, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.3.3)
8. risk scenario development tools and techniques (T1.1.3, 1.1.4, 1.1.5, 1.2.1, 1.2.2, 1.2.3, 1.3.3)
9. risk identification and classification standards, and frameworks (T1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.3.2)
10. risk events/incident concepts (e.g., contributing conditions, lessons learned, loss result) (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6)
11. elements of a risk register (T1.1.5, 1.2.1, 1.2.2, 1.2.3, 1.2.6, 1.3.6)
12. risk appetite and tolerance (T1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.3.3)
13. risk analysis methodologies (quantitative and qualitative) (T1.2.1, 1.2.2, 1.2.3, 1.3.3)
14. organizational structures (T1.1.1, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.4)
15. organizational culture, ethics and behavior (T1.1.1, 1.1.4, 1.1.7, 1.2.1, 1.2.4, 1.2.5, 1.3.1, 1.3.4)

16. organizational assets (e.g., people, technology, data, trademarks, intellectual property) and business processes, including enterprise risk management (ERM) (T1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.3.1)
17. organizational policies and standards (T1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.2.3, 1.2.4, 1.3.1)
18. business process review tools and techniques (T1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.3.5)
19. analysis techniques (e.g., root cause, gap, cost-benefit, return on investment [ROI]) (T1.2.1, 1.2.2, 1.2.3)
20. capability assessment models and improvement techniques and strategies (T1.2.2, 1.2.3, 1.4.4)
21. data analysis, validation and aggregation techniques (e.g., trend analysis, modeling) (T1.2.1, 1.2.2, 1.2.3, 1.4.1, 1.4.2, 1.4.4, 1.4.5)
22. data collection and extraction tools and techniques (T1.1.1, 1.1.2, 1.2.1, 1.3.1, 1.4.1, 1.4.2, 1.4.4, 1.4.5)
23. principles of risk and control ownership (T1.1.4, 1.2.1, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.4, 1.3.5)
24. characteristics of inherent and residual risk (T1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.3.3, 1.4.1, 1.4.2, 1.4.4, 1.4.5)
25. exception management practices (T1.2.1, 1.2.2)
26. risk assessment standards, frameworks and techniques (T1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6)
27. risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection (T1.2.1, 1.2.2, 1.2.3, 1.2.5, 1.3.1, 1.3.3, 1.3.6, 1.3.7)
28. information security concepts and principles, including confidentiality, integrity and availability of information (T1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.2.2, 1.2.3, 1.2.5)
29. systems control design and implementation, including testing methodologies and practices (T1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.2.2, 1.3.3, 1.3.5, 1.4.6)
30. the impact of emerging technologies on design and implementation of controls (T1.2.1, 1.2.2, 1.3.3, 1.3.5)
31. requirements, principles, and practices for educating and training on risk and control activities (T1.1.7, 1.2.5)
32. key risk indicators (KRIs) (T1.2.1, 1.2.2, 1.2.3, 1.4.1, 1.4.2)
33. risk monitoring standards and frameworks (T1.4.1, 1.4.2)
34. risk monitoring tools and techniques (T1.4.1, 1.4.2)
35. risk reporting tools and techniques (T1.2.4, 1.2.5, 1.4.3, 1.4.7)
36. IT risk management best practices (T1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6)
37. key performance indicator (KPIs) (T1.2.1, 1.2.2, 1.2.3, 1.4.4, 1.4.5)
38. control types, standards, and frameworks (T1.2.2, 1.2.3, 1.4.4, 1.4.5)
39. control monitoring and reporting tools and techniques (T1.2.2, 1.2.3, 1.4.4, 1.4.5, 1.4.7)

40. control assessment types (e.g., self-assessments, audits, vulnerability assessments, penetration tests, third-party assurance) (T1.2.1, 1.2.2, 1.2.3, 1.4.6)
41. control activities, objectives, practices and metrics related to:
    - 41.1. business processes (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.2. information security, including technology certification and accreditation practices (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.3. third-party management, including service delivery (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.4. data management (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.5. the system development life cycle (SDLC) (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.6. project and program management (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.7. business continuity and disaster recovery management (DRM) (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.8. IT operations management (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)
    - 41.9. the information systems architecture (e.g., platforms, networks, applications, databases and operating systems) (T1.2.2, 1.2.3, 1.3.3, 1.3.5, 1.4.4, 1.4.5)

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 CRISC concept at the appropriate experience level of the test candidate?

2. Does the item test only one CRISC 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 should not have to make assumptions to answer the question correctly.

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 distractors but only one correct answer?

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

9. Does the item avoid subjective terms such as "frequently," "often," "common"…. in the stem and options?

10. Does the item avoid absolute terms such as "all," "never," "always"… in the stem and options?

11. Does the item avoid such terms as "least," "not," "except"…?