



CRISC® ITEM DEVELOPMENT GUIDE



CRISC ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

<i>Content</i>	<i>Page</i>
Purpose of the CRISC Item Development Guide	3
CRISC Exam Structure	3
Writing Quality Items	3
Multiple-Choice Items	4
Steps to Writing Items	5
General Item Writing Principles	6
Item Examples	7
What to Avoid when Writing Items	8
CRISC Job Practice – What is it?	10
Rubricing	10
Item Submission & Review Process	10
Appendix A: CRISC Job Practice	11
Appendix B: Item Development Checklist	19
Appendix C: Item Construction Form	20

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 also includes Item Writing Principles to assist item writers in becoming more proficient in developing 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

ISACA conducted a CRISC job practice study to determine the tasks and knowledge currently required of IT and business professionals who are responsible for analyzing, evaluating, monitoring and responding to risk and for the design, implementation, monitoring and maintenance of IS controls to mitigate risk factors. The result of this analysis is the CRISC Job Practice, which serves as the blueprint for the CRISC exam. Questions must be written to test a candidate's knowledge of established content areas 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. Items should be developed for individuals with a minimum of 3 years experience performing the tasks outlined within the CRISC Job Practice. One must also consider that the CRISC exam will be administered globally and items need to reflect the international IT and business community. This will require 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.

CRISC ITEM DEVELOPMENT GUIDE

MULTIPLE-CHOICE ITEMS

The CRISC exam consists of 200 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 accepted since they unfairly force test takers to reverse their thinking patterns. 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 distracters. 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.

Distracters:

Distracters 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, practical-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, 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 explanation 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 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.

CRISC ITEM DEVELOPMENT GUIDE

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 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. 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.
7. Items testing knowledge regarding vendor specific products will be returned to the item writer as ISACA does not endorse any vendor products.

CRISC ITEM DEVELOPMENT GUIDE

8. Items will not be accepted if they list specific standards, frameworks, manuals (i.e., COBIT, THE RISK IT PRACTITIONER GUIDE) by name. It is, however, perfectly acceptable and encouraged to test the knowledge associated with these best practices.
9. 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. Any concept tested must be an accepted and recognized practice globally and in all industries.

ITEM EXAMPLES

Items can either be direct questions, incomplete statements or scenario questions.

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 doing so offers smoother, less repetitive wording.

CRISC ITEM DEVELOPMENT GUIDE

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 and practical, and it must 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 can not 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 since you can explain the specifics requirements of the regulation or the organization's reporting structure in the introductory paragraph(s).

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.

CRISC ITEM DEVELOPMENT GUIDE

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 because 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 or rewritten because the word “prevention” in the stem points to “prevents” in Option A, making the answer (key) too obvious.

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 tasks and corresponding knowledge will be the basis for CRISC exam questions. The goal of the CRISC exam is to write practice-based questions testing knowledge necessary to perform a task. The CRISC Job Practice can be found in Appendix A. To assist you in writing questions, we have indicated the related task statement(s) after each knowledge statement. Remember, when developing an item, the focus should be on one knowledge statement or testing concept.

RUBRICING

All items must be assigned a rubric. The rubric indicates which CRISC task and knowledge statement is most closely associated with the item. 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—CRISC JOB PRACTICE when rubricing an item.

ITEM SUBMISSION AND REVIEW PROCESS

Items must be submitted to CRISCitems@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.**

All subject matter experts that have completed the *CRISC Item Writing Application* will receive periodic emails (item writing campaigns) communicating the task and knowledge statements within the CRISC Job Practice that are requested by the CRISC Certification Committee. Item writing campaigns will also include submission deadlines.

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 CRISC Test Enhancement Subcommittee (TES) to be considered for inclusion in the exam item pool.

Once reviewed by the TES, the item will be accepted or returned. If returned by the TES, 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 the areas of need will be awarded US \$50.00.

CRISC ITEM DEVELOPMENT GUIDE

Appendix A

CRISC JOB PRACTICE

NOTE: The highlighted task and knowledge statements tend to be subjective content making them difficult to write globally accepted questions with only one answer. We encourage item writers to develop scenario questions to test these subjective areas. Scenario questions allow the item writer to include subjective information and specifics in the introductory paragraphs so no assumptions need to be made to answer the question. For example, when testing roles and responsibilities, an organization chart and specific roles and responsibilities can be defined in the scenario. Multiple questions can then be written to test the information included in the scenario.

Please note that the digits at the end of the knowledge statement represent the task that those knowledge statements map to. For example, to perform the task listed in task statement 1.1, an individual will need to have the knowledge indicated in knowledge statements 1.1, 1.2 or 1.3.

Domain 1—Risk Identification, Assessment and Evaluation: Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.

Task Statements

- 1.1 Collect information and review documentation to ensure that risk scenarios are identified and evaluated.
- 1.2 Identify legal, regulatory and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.
- 1.3 Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
- 1.4 Create and maintain a risk register to ensure that all identified risk factors are accounted for.
- 1.5 Assemble risk scenarios to estimate the likelihood and impact of significant events to the organization.
- 1.6 Analyze risk scenarios to determine their impact on business objectives.
- 1.7 Develop a risk awareness program and conduct training to ensure that stakeholders understand risk and contribute to the risk management process and to promote a risk-aware culture.
- 1.8 Correlate identified risk scenarios to relevant business processes to assist in identifying risk ownership.
- 1.9 Validate risk appetite and tolerance with senior leadership and key stakeholders to ensure alignment.

Knowledge Statements

- 1.1 Knowledge of standards, frameworks and leading practices related to risk identification, assessment and evaluation [1.1, 1.3, 1.5, 1.6, 1.9]
- 1.2 Knowledge of techniques for risk identification, classification, assessment and evaluation [1.1, 1.6]

CRISC ITEM DEVELOPMENT GUIDE

- 1.3 Knowledge of quantitative and qualitative risk evaluation methods [1.1]
- 1.4 Knowledge of business goals and objectives [1.2, 1.6]
- 1.5 Knowledge of organizational structures [1.2, 1.6, 1.7]
- 1.6 Knowledge of risk scenarios related to business processes and initiatives [1.2, 1.7, 1.3, 1.6]
- 1.7 Knowledge of business information criteria [1.2, 1.5, 1.6]
- 1.8 Knowledge of threats and vulnerabilities related to business processes and initiatives [1.5, 1.6, 1.7, 1.3]
- 1.9 Knowledge of information systems architecture (e.g. platforms, networks, applications, databases and operating systems) [1.5, 1.6]
- 1.10 Knowledge of information security concepts [1.2, 1.5, 1.6, 1.7]
- 1.11 Knowledge of threats and vulnerabilities related to third-party management [1.2, 1.6, 1.7]
- 1.12 Knowledge of threats and vulnerabilities related to data management [1.2, 1.6, 1.7]
- 1.13 Knowledge of threats and vulnerabilities related to the system development life cycle [1.2, 1.6, 1.7]
- 1.14 Knowledge of threats and vulnerabilities related to project and program management [1.2, 1.6, 1.7]
- 1.15 Knowledge of threats and vulnerabilities related to business continuity and disaster recovery management [1.2, 1.6, 1.7]
- 1.16 Knowledge of threats and vulnerabilities related to management of IT operations [1.6, 1.7]
- 1.17 Knowledge of the elements of a risk register [1.3, 1.4]
- 1.18 Knowledge of risk scenario development tools and techniques [1.5, 1.6]
- 1.19 Knowledge of risk awareness training tools and techniques [1.7]
- 1.20 Knowledge of principles of risk ownership [1.8]
- 1.21 Knowledge of current and forthcoming laws, regulations and standards [1.2]
- 1.22 Knowledge of threats and vulnerabilities associated with emerging technologies [1.1, 1.3]

CRISC ITEM DEVELOPMENT GUIDE

Domain 2—Risk Response: Develop and implement risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives.

Task Statements

- 2.1 Identify and evaluate risk response options and provide management with information to enable risk response decisions.
- 2.2 Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy.
- 2.3 Apply risk criteria to assist in the development of the risk profile for management approval.
- 2.4 Assist in the development of risk response action plans to address risk factors identified in the organizational risk profile.
- 2.5 Assist in the development of business cases supporting the investment plan to ensure risk responses are aligned with the identified business objectives.

Knowledge Statements

- 2.1 Knowledge of standards, frameworks and leading practices related to risk response [2.1, 2.2, 2.3, 2.4]
- 2.2 Knowledge of risk response options [2.1, 2.2]
- 2.3 Knowledge of cost-benefit analysis and return on investment (ROI) [2.1, 2.2]
- 2.4 Knowledge of risk appetite and tolerance [2.1, 2.2, 2.5]
- 2.5 Knowledge of organizational risk management policies [2.1, 2.3]
- 2.6 Knowledge of parameters for risk response selection [2.2, 2.3]
- 2.7 Knowledge of project management tools and techniques [2.3]
- 2.8 Knowledge of portfolio, investment and value management [2.1, 2.2, 2.3, 2.4]
- 2.9 Knowledge of exception management [2.2]
- 2.10 Knowledge of residual risk [2.1, 2.2, 2.4, 2.5]

CRISC ITEM DEVELOPMENT GUIDE

Domain 3—Risk Monitoring: Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise’s risk management strategy.

Task Statements

- 3.1 Collect and validate data that measure key risk indicators (KRIs) to monitor and communicate their status to relevant stakeholders.
- 3.2 Monitor and communicate key risk indicators (KRIs) and management activities to assist relevant stakeholders in their decision-making process.
- 3.3 Facilitate independent risk assessments and risk management process reviews to ensure that they are performed efficiently and effectively.
- 3.4 Identify and report on risk, including compliance, to initiate corrective action and meet business and regulatory requirements.

Knowledge Statements

- 3.1 Knowledge of standards, frameworks and leading practices related to risk monitoring [3.1, 3.2, 3.3, 3.4]
- 3.2 Knowledge of principles of risk ownership [3.1, 3.2]
- 3.3 Knowledge of risk and compliance reporting requirements, tools and techniques [3.1, 3.2, 3.3, 3.4]
- 3.4 Knowledge of key performance indicators (KPIs) and key risk indicators (KRIs) [3.1, 3.2, 3.3]
- 3.5 Knowledge of risk assessment methodologies [3.1, 3.2, 3.3, 3.4]
- 3.6 Knowledge of data extraction, validation, aggregation and analysis tools and techniques [3.1, 3.2]
- 3.7 Knowledge of various types of reviews of the organization’s risk monitoring process (e.g., internal and external audits, peer reviews, regulatory reviews, quality reviews) [3.4]

CRISC ITEM DEVELOPMENT GUIDE

Domain 4—Information Systems Control Design and Implementation: Design and implement information systems controls in alignment with the organization’s risk appetite and tolerance levels to support business objectives.

Task Statements

- 4.1 Interview process owners and review process design documentation to gain an understanding of the business process objectives.
- 4.2 Analyze and document business process objectives and design to identify required information systems controls.
- 4.3 Design information systems controls in consultation with process owners to ensure alignment with business needs and objectives.
- 4.4 Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
- 4.5 Monitor the information systems control design and implementation process to ensure that it is implemented effectively and within time, budget and scope.
- 4.6 Provide progress reports on the implementation of information systems controls to inform stakeholders and to ensure that deviations are promptly addressed.
- 4.7 Test information systems controls to verify effectiveness and efficiency prior to implementation.
- 4.8 Implement information systems controls to mitigate risk.
- 4.9 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of information systems control performance in meeting business objectives.
- 4.10 Assess and recommend tools to automate information systems control processes.
- 4.11 Provide documentation and training to ensure that information systems controls are effectively performed.
- 4.12 Ensure that all controls are assigned control owners to establish accountability.
- 4.13 Establish control criteria to enable control life cycle management.

Knowledge Statements

- 4.1 Knowledge of standards, frameworks and leading practices related to information systems control design and implementation [4.2, 4.3, 4.5, 4.8, 4.9, 4.12, 4.13]
- 4.2 Knowledge of business process review tools and techniques [4.1]
- 4.3 Knowledge of testing methodologies and practices related to information systems control design and implementation [4.3, 4.7]
- 4.4 Knowledge of control practices related to business processes and initiatives [4.1, 4.3, 4.8, 4.9, 4.11]
- 4.5 Knowledge of the information systems architecture (e.g., platforms, networks, applications, databases and operating systems) [4.1, 4.2, 4.3, 4.8]
- 4.6 Knowledge of controls related to information security [4.1, 4.3, 4.4, 4.8]
- 4.7 Knowledge of controls related to third-party management [4.1, 4.3, 4.4, 4.8]
- 4.8 Knowledge of controls related to data management [4.1, 4.3, 4.4, 4.8]
- 4.9 Knowledge of controls related to the system development life cycle [4.1, 4.3, 4.4, 4.8, 4.13]
- 4.10 Knowledge of controls related to project and program management [4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.11, 4.12]

CRISC ITEM DEVELOPMENT GUIDE

- 4.11 Knowledge of controls related to business continuity and disaster recovery management [4.1, 4.2, 4.3, 4.4, 4.8]
- 4.12 Knowledge of controls related to management of IT operations [4.1, 4.3, 4.4]
- 4.13 Knowledge of software and hardware certification and accreditation practices [4.1, 4.3, 4.4]
- 4.14 Knowledge of the concept of control objectives [4.2, 4.7, 4.8, 4.9, 4.13]
- 4.15 Knowledge of governance, risk and compliance (GRC) tools [4.9, 4.10]
- 4.16 Knowledge of tools and techniques to educate and train users [4.2, 4.11]

CRISC ITEM DEVELOPMENT GUIDE

Domain 5—Information Systems Control Monitoring and Maintenance: Monitor and maintain information systems controls to ensure they function effectively and efficiently.

Task Statements

- 5.1 Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls.
- 5.2 Collect information and review documentation to identify information systems control deficiencies.
- 5.3 Review information systems policies, standards and procedures to verify that they address the enterprise's internal and external requirements.
- 5.4 Assess and recommend tools and techniques to automate information systems control verification processes.
- 5.5 Evaluate the current state of information systems processes using a maturity model to identify the gaps between current and targeted process maturity.
- 5.6 Determine approach to correct information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately considered and remediated.
- 5.7 Maintain sufficient, adequate evidence to support conclusions on the existence and operating effectiveness of information systems controls.
- 5.8 Provide information systems control status reporting to relevant stakeholders to enable informed decision making.

Knowledge Statements

- 5.1 Knowledge of standards, frameworks and leading practices related to information systems control monitoring and maintenance [5.1, 5.2, 5.3, 5.7, 5.8]
- 5.2 Knowledge of enterprise security architecture [5.1, 5.2, 5.3]
- 5.3 Knowledge of monitoring tools and techniques [5.1, 5.2, 5.3, 5.4, 5.7, 5.8]
- 5.4 Knowledge of maturity models [5.5, 5.6, 5.8]
- 5.5 Knowledge of control objectives, activities and metrics related to IT operations and business processes and initiatives [5.1, 5.2, 5.3]
- 5.6 Knowledge of control objectives, activities and metrics related to incident and problem management [5.1, 5.2, 5.3]
- 5.7 Knowledge of security testing and assessment tools and techniques [5.1, 5.2, 5.3, 5.4]
- 5.8 Knowledge of control objectives, activities and metrics related to information systems architecture (platforms, networks, applications, databases and operating systems) [5.1, 5.2, 5.3]
- 5.9 Knowledge of control objectives, activities and metrics related to information security [5.1, 5.2, 5.3]
- 5.10 Knowledge of control objectives, activities and metrics related to third-party management [5.1, 5.2, 5.3]
- 5.11 Knowledge of control objectives, activities and metrics related to data management [5.1, 5.2, 5.3]
- 5.12 Knowledge of control objectives, activities and metrics related to the system development life cycle [5.1, 5.2, 5.3]

CRISC ITEM DEVELOPMENT GUIDE

- 5.13 Knowledge of control objectives, activities and metrics related to project and program management [5.1, 5.2, 5.3]
- 5.14 Knowledge of control objectives, activities and metrics related to software and hardware certification and accreditation practices [5.1, 5.2, 5.3]
- 5.15 Knowledge of control objectives, activities and metrics related to business continuity and disaster recovery management [5.1, 5.2, 5.3]
- 5.16 Knowledge of applicable laws and regulations [5.3]

CRISC ITEM DEVELOPMENT GUIDE

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 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, if the stem includes: "Which of the following controls...", then 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 negative terms such as "least," "not," or "except" in the stem?

CRISC ITEM DEVELOPMENT GUIDE

Appendix C

ITEM CONSTRUCTION FORM

Name:

Task Statement: *(Refer to CRISC Job Practice) This is mandatory; any items submitted without a task statement will be returned*

Knowledge Statement: *(Refer to CRISC 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: Provide references to enable independent review. Include the publication title, publication year, author and page.