CRISC™ QAE ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

CRISC QAE ITEM DEVELOPMENT GUIDE

PURPOSE OF THE CRISC QAE ITEM DEVELOPMENT GUIDE

The purpose of the CRISC™Item Development Guide (Guide) is to provide assistance to item writers in their efforts to develop items for the *CRISC™Review Questions, Answers & Explanations* (QAE) *Manual.* This Guide explains the structure of CRISC 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 CRISC QAE

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

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 implementation and monitoring 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

The first thing to consider when writing an item is its 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. 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 will require the item writer to be somewhat flexible when determining a globally accepted practice.

Note that items submitted for consideration by the CRISC 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 CRISC QAT and vice versa.

CRISC TERMINOLOGY

Because foundational terms such as risk, threat and vulnerability 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.

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 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 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, practice-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 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. Please note that Wikipedia is not an applicable reference.

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.
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.

8. Items will not be accepted if they list specific standards, frameworks or manuals (i.e., COBIT, ISO, ITIL, etc.) 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 concepts tested must be accepted and recognized practice globally and in all industries.

ITEM EXAMPLES

Please note that the item examples appearing in this Guide have been taken from other exam study sources and are included here only as examples of exam item format (not content) to help you construct your CRISC items.

Items can 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.

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 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 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 since you can explain the specifics requirements of the regulation or the organization's reporting structure in the introductory paragraph(s).

When writing items associated with the scenario, ask yourself if the item could be answered **without** reading the scenario. If the answer is yes, it will most likely not be accepted as a scenario item and may be better as a "stand alone" item. It is equally important that the scenario and corresponding items are written to test a candidate's knowledge and experience. If the scenario is written merely as a reading exercise and

answers can be found within the scenario itself, it is not a strong scenario and will most likely be returned. Due to the complexities of writing scenarios, we would encourage item writers to gain some experience in writing items before working on a scenario.

WHAT TO AVOID WHEN CONSTRUCTING ITEMS

Following are items to illustrate what to avoid when constructing quality 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 because Option D directly relates to Option A and therefore could be keyable. Option C is not understandable. We would also advise the item writer to try to make all options more parallel in length.

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 it 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 JOB PRACTICE – WHAT IS IT?

The CRISC Job Practice lists the relevant tasks performed by IT professionals working in the areas of IS audit and control and the knowledge necessary to perform those tasks. These tasks and 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. 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 2 to 3-digit task statement number AND a 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

All subject matter experts that have indicated an interest in CRISC 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 CRISCQAE@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 CRISC Quality Assurance Team (QAT) to be considered for inclusion in the *CRISC® Review Questions, Answers & Explanations* (QAE) *Manual.*

Once reviewed by the CRISC 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 CRISC 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 CRISC QAT and vice versa.

Appendix A
CRISC Job Practice

Domain 1—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 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.
1.2 Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis.
1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.
1.4 Identify key stakeholders for IT risk scenarios to help establish accountability.
1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.
1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
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.

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.
2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
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.

3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
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).
3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
3.4 Ensure that control ownership is assigned to establish clear lines of accountability.
3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
3.6 Update the risk register to reflect changes in risk and management's risk response.
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.

4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
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.
4.6 Review the results of control assessments to determine the effectiveness of the control environment.
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 QAE ITEM DEVELOPMENT GUIDE

CRISC Knowledge Statements

Knowledge of:

1. laws, regulations, standards and compliance requirements
2. industry trends and emerging technologies
3. enterprise systems architecture (e.g., platforms, networks, applications, databases and operating systems)
4. business goals and objectives
5. contractual requirements with customers and third-party service providers
6. threats and vulnerabilities related to:
   6.1. business processes and initiatives
   6.2. third-party management
   6.3. data management
   6.4. hardware, software and appliances
   6.5. the system development life cycle (SDLC)
   6.6. project and program management
   6.7. business continuity and disaster recovery management (DRM)
   6.8. management of IT operations
   6.9. emerging technologies
7. methods to identify risk
8. risk scenario development tools and techniques
9. risk identification and classification standards, and frameworks
10. risk events/incident concepts (e.g., contributing conditions, lessons learned, loss result)
11. elements of a risk register
12. risk appetite and tolerance
13. risk analysis methodologies (quantitative and qualitative)
14. organizational structures
15. organizational culture, ethics and behavior
16. organizational assets (e.g., people, technology, data, trademarks, intellectual property) and business processes, including enterprise risk management (ERM)
17. organizational policies and standards
18. business process review tools and techniques
19. analysis techniques (e.g., root cause, gap, cost-benefit, return on investment [ROI])
20. capability assessment models and improvement techniques and strategies
21. data analysis, validation and aggregation techniques (e.g., trend analysis, modeling)
22. data collection and extraction tools and techniques
23. principles of risk and control ownership
24. characteristics of inherent and residual risk
25. exception management practices
26. risk assessment standards, frameworks and techniques
27. risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection
28. information security concepts and principles, including confidentiality, integrity and availability of information

29. systems control design and implementation, including testing methodologies and practices
30. the impact of emerging technologies on design and implementation of controls
31. requirements, principles, and practices for educating and training on risk and control activities
32. key risk indicators (KRIs)
33. risk monitoring standards and frameworks
34. risk monitoring tools and techniques
35. risk reporting tools and techniques
36. IT risk management best practices
37. key performance indicator (KPIs)
38. control types, standards, and frameworks
39. control monitoring and reporting tools and techniques
40. control assessment types (e.g., self-assessments, audits, vulnerability assessments, penetration tests, third-party assurance)
41. control activities, objectives, practices and metrics related to:
    - 41.1. business processes
    - 41.2. information security, including technology certification and accreditation practices
    - 41.3. third-party management, including service delivery
    - 41.4. data management
    - 41.5. the system development life cycle (SDLC)
    - 41.6. project and program management
    - 41.7. business continuity and disaster recovery management (DRM)
    - 41.8. IT operations management
    - 41.9. the information systems architecture (e.g., platforms, networks, applications, databases and operating systems)

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: "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" or "except" in the stem?

12. Does the item avoid "multiple-multiple" choices within the options?

Appendix C

ITEM CONSTRUCTION FORM

Name:
ISACA ID:
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: *Justifications for all options are mandatory; any items submitted without justifications will be returned.*
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. *This is mandatory; any items submitted without a reference will be returned.*