CISA® QAE ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

PURPOSE OF THE CISA QAE ITEM DEVELOPMENT GUIDE

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

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

CISA EXAM STRUCTURE

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

WRITING QUALITY ITEMS

The first thing to consider when writing an item is its target audience, or the CISA exam candidate. An item must be developed at the proper level of experience expected of a successful CISA candidate. This level of experience, as defined by the CISA Certification Board, is as follows:

> "*A CISA should have the ability to autonomously perform the specifics of their role as part of a team, seeking or taking direction where necessary, but acting proactively otherwise. CISAs should have sufficient knowledge and experience to be able to plan their work, make judgments about the relative importance of issues in terms of the business environment, manage assignments and needs effectively, and redevelop plans where necessary. A CISA would normally work for, take direction from more proficient staff members or managers and would seek assistance on complex technology issues from technical experts.*"

While writing items, one must take into consideration that IS audit and control is a global profession, and individual perceptions and experiences might not reflect the more global position or circumstance. Since the examination and CISA items are developed for the international IS audit and control 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 CISA 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 CISA QAT and vice versa.

MULTIPLE-CHOICE ITEMS

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

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

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

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

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

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

STEPS TO WRITING ITEMS

STEP 1 Select a topic within the CISA 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 "CISA Job Practice" for a list of the task and related knowledge statements.

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

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

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

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

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

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

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

GENERAL ITEM WRITING PRINCIPLES

DOs:

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

DON'Ts:

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

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

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

ITEM EXAMPLES

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

Direct question:

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

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

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

Incomplete statement:

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

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

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

SCENARIO QUESTIONS

There are a number of considerations when writing scenario questions.

This type of item consists of introductory information (or the scenario) for the items to follow.

- There should be a set of two-to-five items that pertain to this introductory information.
- The introductory material must be related to a particular field, be relevant 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 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).

WHAT TO AVOID WHEN CONSTRUCTING ITEMS

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

Example 1:

Stem: An IS auditor is reviewing an organization's disaster recovery plan. Which of the following areas should the auditor review?

Options:
A. Offsite data file storage
B. Firefighting equipment
C. Backup UPS for the computer center
D. Access to the data center by backup staff

Key: A

All options could be correct. There is not enough information in the stem to be able to choose only one correct answer. An IS auditor should look at all options when reviewing a disaster recovery plan.

Example 2:

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

The stem assumes functional responsibility. The CISA 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 3:

Stem: Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job costing system. What is the **BEST** control to ensure that data entered into the job costing system is accurate?

Options:
A. Reconciliation of total amounts by project.
B. Reasonableness of total amounts by project.
C. Validity checks, preventing entry of character data.
D. Display back of project detail after entry

Key: A

Can a non-IS auditor answer this question? Does this question test an IS audit concept? There are some questions that IS auditors need to be tested on. This is a borderline concept. For the most part, we encourage strictly IS audit concepts.

CISA JOB PRACTICE – WHAT IS IT?

The CISA 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 CISA exam questions. The goal of the CISA exam is to write practice-based questions testing knowledge necessary to perform a task. The CISA 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 CISA task and knowledge statement the item most closely refers to. Each rubric consists of a 2 to 3-digit task statement number AND a 2 to 3-digit knowledge statement number. The rubrics are indicated before each task and knowledge statement. Please refer to Appendix A—CISA JOB PRACTICE when rubricing an item.

ITEM SUBMISSION AND REVIEW PROCESS

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

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

Appendix A
CISA Job Practice

Domain 1 – The Process of Auditing Information Systems: Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems.

Task Statements:

1.1 Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
1.2 Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
1.3 Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
1.4 Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
1.5 Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.

Knowledge Statements:

KS1.1 Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards [1.1, 1.2, 1.3, 1.4, 1.5]
KS1.2 Knowledge of risk assessment concepts, tools and techniques in an audit context [1.1, 1.2]
KS1.3 Knowledge of control objectives and controls related to information systems [1.2, 1.3]
KS1.4 Knowledge of audit planning and audit project management techniques, including follow- up [1.2, 1.3, 1.5]
KS1.5 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT [1.2, 1.3]
KS1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits [1.1, 1.2, 1.3, 1.4]
KS1.7 Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis) used to gather, protect and preserve audit evidence [1.3]
KS1.8 Knowledge of different sampling methodologies [1.2, 1.3]
KS1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure) [1.4, 1.5]
KS1.10 Knowledge of audit quality assurance systems and frameworks [1.3]

Domain 2 – Governance and Management of IT: Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy.

Task Statements:

2.1 Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
2.2 Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
2.3 Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
2.4 Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
2.5 Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
2.6 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures.
2.7 Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.
2.8 Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.
2.9 Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.
2.10 Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
2.11 Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

Knowledge Statements:

KS2.1 Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines, and practices [2.1, 2.4, 2.6]
KS2.2 Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each [2.3, 2.4]
KS2.3 Knowledge of organizational structure, roles and responsibilities related to IT [2.6, 2.7]
KS2.4 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
KS2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions [2.3]
KS2.6 Knowledge of relevant laws, regulations and industry standards affecting the organization [2.4]
KS2.7 Knowledge of quality management systems [2.4, 2.5]
KS2.8 Knowledge of the use of maturity models [2.6, 2.9, 2.10]
KS2.9 Knowledge of process optimization techniques [2.5, 2.6, 2.7]
KS2.10 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management) [2.7]

KS2.11 Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships [2.1, 2.3, 2.8]
KS2.12 Knowledge of enterprise risk management [2.2, 2.4, 2.9]
KS2.13 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI]) [2.6, 2.10]
KS2.14 Knowledge of IT human resources (personnel) management practices used to invoke the business continuity plan [2.2, 2.11]
KS2.15 Knowledge of business impact analysis (BIA) related to business continuity planning [2.11]
KS2.16 Knowledge of the standards and procedures for the development and maintenance of the business continuity plan and testing methods [2.11]

Domain 3 – Information Systems Acquisition, Development and Implementation: Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

Task Statements:

3.1 Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
3.2 Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
3.3 Conduct reviews to determine whether a project is progressing in accordance with project plans is adequately supported by documentation and status reporting is accurate.
3.4 Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
3.5 Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls, and organization's requirements are met.
3.6 Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and organization's requirements are met.

Knowledge Statements:

KS3.1 Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], ROI) [3.1, 3.2]
KS3.2 Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office) [3.2]
KS3.3 Knowledge of project management control frameworks, practices and tools [3.2]
KS3.4 Knowledge of risk management practices applied to projects [3.2, 3.3]
KS3.5 Knowledge of IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications) [3.1]
KS3.6 Knowledge of acquisition practices (e.g., evaluation of vendors, vendor management, escrow) [3.1, 3.5]
KS3.7 Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements) [3.2, 3.5]
KS3.8 3.8 Knowledge of project success criteria and risks [3.2, 3.3]
KS3.9 Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data [3.4]
KS3.10 Knowledge of system development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques) [3.2, 3.4]
KS3.11 Knowledge of testing methodologies and practices related to information systems development [3.4]
KS3.12 Knowledge of configuration and release management relating to the development of information systems [3.4, 3.5]
KS3.13 Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures [3.4, 3.5]
KS3.14 Knowledge of post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement) [3.6]

Domain 4 – Information Systems Operations, Maintenance and Support – Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

Task Statements:

4.1 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
4.2 Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
4.3 Evaluate third party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
4.4 Evaluate operations and end-user procedures to determine whether scheduled and non-scheduled processes are managed to completion.
4.5 Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
4.6 Evaluate data administration practices to determine the integrity and optimization of databases.
4.7 Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives.
4.8 Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
4.9 Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the organization's production environment are adequately controlled and documented.
4.10 Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing.
4.11 Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

Knowledge Statements:

KS4.1 Knowledge of service level management practices and the components within a service level agreement [4.2]
KS4.2 Knowledge of techniques for monitoring third party compliance with the organization's internal controls [4.3]
KS4.3 Knowledge of operations and end-user procedures for managing scheduled and non-scheduled processes [4.3]
KS4.4 Knowledge of the technology concepts related to hardware and network components, system software and database management systems [4.5, 4.6]
KS4.5 Knowledge of control techniques that ensure the integrity of system interfaces [4.5, 4.9]
KS4.6 Knowledge of software licensing and inventory practices [4.5]
KS4.7 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering) [4.5]
KS4.8 Knowledge of database administration practices [4.6]
KS4.9 Knowledge of capacity planning and related monitoring tools and techniques [4.7]
KS4.10 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing) [4.7]
KS4.11 Knowledge of problem and incident management practices (e.g., help desk, escalation procedures, tracking) [4.8]

KS4.12 Knowledge of processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices [4.9]
KS4.13 Knowledge of data backup, storage, maintenance, retention and restoration practices [4.10]
KS4.14 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery [4.11]
KS4.15 Knowledge of business impact analysis (BIA) related to disaster recovery planning [4.11]
KS4.16 Knowledge of the development and maintenance of disaster recovery plans [4.10, 4.11]
KS4.17 Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites) [4.11]
KS4.18 Knowledge of processes used to invoke the disaster recovery plans [4.11]
KS4.19 Knowledge of disaster recovery testing methods [4.10, 4.11]

Domain 5 – Protection of Information Assets: Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

Task Statements:

5.1 Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
5.2 Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
5.3 Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.
5.4 Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

Knowledge Statements:

KS5.1 Knowledge of the techniques for the design, implementation, and monitoring of security controls, including security awareness programs [5.1, 5.2, 5.3, 5.4, 5.5]
KS5.2 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team) [5.1]
KS5.3 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data [5.2]
KS5.4 Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems), and database management systems [5.2]
KS5.5 Knowledge of risks and controls associated with virtualization of systems [5.2, 5.4]
KS5.6 Knowledge of the configuration, implementation, operation and maintenance of network security controls [5.2]
KS5.7 Knowledge of network and Internet security devices, protocols, and techniques [5.2]
KS5.8 Knowledge of information system attack methods and techniques [5.2, 5.4]
KS5.9 Knowledge of detection tools and control techniques (e.g., malware, virus detection, spyware) [5.2]
KS5.10 Knowledge of security testing techniques (e.g., intrusion testing, vulnerability scanning) [5.2]
KS5.11 Knowledge of risks and controls associated with data leakage [5.2, 5.3, 5.4]
KS5.12 Knowledge of encryption-related techniques [5.2, 5.3, 5.5]
KS5.13 Knowledge of public key infrastructure (PKI) components and digital signature techniques [5.2, 5.3, 5.5]
KS5.14 Knowledge of risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs) [5.2]
KS5.15 Knowledge of controls and risks associated with the use of mobile & wireless devices [5.2]
KS5.16 Knowledge of voice communications security (e.g., PBX, VoIP) [5.2, 5.4]
KS5.17 Knowledge of the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody) [5.2]
KS5.18 Knowledge of data classification standards and supporting procedures [5.3, 5.5]

KS5.19 Knowledge of physical access controls for the identification, authentication and restriction of users to authorized facilities [5.4]
KS5.20 Knowledge of environmental protection devices and supporting practices [5.4]
KS5.21 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets [5.3, 5.5]

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

2. Does the item test only one CISA 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"?

Appendix C

ITEM CONSTRUCTION FORM

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

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

Stem:

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

Key: A

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

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

