CISM® ITEM DEVELOPMENT GUIDE
# CISM ITEM DEVELOPMENT GUIDE

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of the CISM Item Development Guide</td>
<td>2</td>
</tr>
<tr>
<td>CISM Exam Structure</td>
<td>2</td>
</tr>
<tr>
<td>Item Writing Campaigns</td>
<td>2</td>
</tr>
<tr>
<td>Why Participate as a CISM Item Writer?</td>
<td>2</td>
</tr>
<tr>
<td>Writing Quality Items</td>
<td>2</td>
</tr>
<tr>
<td>Multiple-Choice Items</td>
<td>3</td>
</tr>
<tr>
<td>Developing an Item</td>
<td>4</td>
</tr>
<tr>
<td>General Item Writing Principles</td>
<td>5</td>
</tr>
<tr>
<td>Item Examples</td>
<td>6</td>
</tr>
<tr>
<td>What to Avoid when Constructing Items</td>
<td>7</td>
</tr>
<tr>
<td>Item Development Form</td>
<td>8</td>
</tr>
<tr>
<td>Item Submission &amp; Review Process</td>
<td>8</td>
</tr>
<tr>
<td>Appendix A: CISM Job Practice Analysis</td>
<td>9</td>
</tr>
<tr>
<td>Appendix B: Item Development Form</td>
<td>15</td>
</tr>
<tr>
<td>Appendix C: Item Development Checklist</td>
<td>16</td>
</tr>
</tbody>
</table>
PURPOSE OF THE CISM ITEM DEVELOPMENT GUIDE
The purpose of this CISM Item Development Guide (Guide) is to provide assistance to item writers in their efforts to increase the quality of new exam items. This Guide thoroughly explains the structure of CISM exam questions and will assist item writers in becoming more skilled in writing and critiquing items.

As you read through this Guide, please pay particular interest to the item writing principles appearing on page 5. Applying these principles will greatly enhance the chances of your items being accepted.

CISM EXAM STRUCTURE
ISACA and the CISM Certification Board periodically perform a CISM Job Practice Analysis study to determine the tasks and knowledge required of today’s and tomorrow’s information security managers. The results of this analysis serve as the blueprint for the CISM examination and the CISM item bank. Questions must be written to test a candidate’s knowledge of established process and content areas defined by the CISM Job Practice Analysis (see Appendix A “CISM Job Practice Analysis” or http://www.isaca.org/CISMcontentareas

ITEM WRITING CAMPAIGNS
ISACA conducts approximately two item writing campaigns per year (spring and fall). The purpose of a campaign is to instruct item writers of the specific areas within the CISM Job Practice to write items. A CISM Test Enhancement Committee (TEC) meeting is scheduled at the conclusion of each item writing campaign to review newly submitted items. All items that are accepted by the CISM TEC are forwarded to the CISM Certification Board for review and possible inclusion on future CISM exams.

WHY PARTICIPATE AS A CISM ITEM WRITER?
As a CISM item writer you will receive the satisfaction of helping to shape the information security profession. In addition, both monetary and continuing education rewards can be gained. CISM item writers receive a US$100 honorarium and 1 continuing education credit hour for each item that meets the item writing campaign requirements and accepted by the CISM TEC. A US $50 honorarium will be awarded for items accepted by the CISM TEC but written outside the campaign areas. Items that are not accepted by the CISM TEC are returned to the item writer with constructive feedback on how to improve the item.

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

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

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

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

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

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

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

Distracters
Distracters are the incorrect options but should be plausible or possible correct answers to candidates who are not knowledgeable enough to choose the key.
DEVELOPING AN ITEM
Item writers must use the Item Development Form included in Appendix B when developing and submitting new items to ISACA. Become familiar with this form prior to item development and make every attempt to complete all sections of the form for each item submitted.

Item writers can write items on any topic within the CISM Job Practice but are encouraged to concentrate the development of items within the areas specified in the CISM item writing campaign. For best results, items should be written on a knowledge statement within a specific task area. Items should focus on a single topic or knowledge statement.

Once a topic is chosen, follow the steps listed below. While writing your item, please refer to the General Item Writing Principles appearing on page 5 for further guidance and review your item with the Item Development Checklist in Appendix C.

STEP 1 – Write the item stem and keyable answer (Answer A on the Item Development Form).

STEP 2 – Develop plausible distracters. The distracters should not be made up words or phrases, but may 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 other subject matter experts.

STEP 3 - 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 4 - If reference texts are used for the development of an item the reference sources should be noted on the Item Development Form. Refer to KNET on the ISACA website for applicable references – http://www.isaca.org/knet

STEP 5 – Review your item using the Item Development Checklist in Appendix C.

STEP 6 - Have a peer or colleague review and critique your item.

STEP 7 – Submit the item to ISACA. (Refer to Item Submission and Review Process on page 8).
GENERAL ITEM WRITING PRINCIPLES

The “DOs and DO NOTs” of Item Writing

DO:
1. DO test only one testing concept or knowledge statement per item. Knowledge statements were developed for this purpose and items written from a knowledge statement will most likely result in higher quality, practically based items. For a listing of knowledge statements, refer to Appendix A - CISM Job Practice Analysis or http://www.isaca.org/CISMcontentareas
2. DO ensure that the stem and all options are compatible with each other. For example, if your stem reads, “Which of the following information security procedures… “, then all options must be information security procedures.
3. DO 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.
4. DO include common words or phrases in the item stem rather than in the key and distracters.
5. DO write all options the same approximate length and format.
6. DO 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.
7. DO use only professionally acceptable or technical terminology in the item stem and options.

DO NOT:
1. DO NOT use 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. DO NOT use words such as “frequently”, “often”, “common”, or “rarely” as they introduce subjectivity into the item. If an item is subjective, it can be argued that more than one option is keyable.
3. DO NOT use terms in the stem such as “always”, “never”, or “all” since very little is absolute and thus it makes it easier for candidates to eliminate distracters.
4. DO NOT use terms such as “least”, “not” or “except” as they are negative and require a candidate to choose an incorrect or least preferred choice, rather than a correct or preferred choice. These questions will be returned to the item writer without TEC review.
5. DO NOT use gender pronouns such as he, she, his, or her. Refer to individuals by their title, such as the information security manager.
6. DO NOT use “all of the above”, “none of the above”, as options. These questions will be returned to the item writer without TEC review.
7. DO NOT test knowledge regarding vendor specific products. These questions will be returned to the item writer without TEC review.
ITEM EXAMPLES

Direct vs Incomplete Statement Items

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

Direct question

Stem: Which of the following types of firewalls would be BEST for an organization where the most important requirement is performance?

Options:
- A. Packet filtering
- B. Stateful inspection
- C. Application level
- D. Circuit

Incomplete statement

Stem: The BEST type of firewall for an organization where the most important requirement is performance is:

Options:
- A. packet filtering.
- B. stateful inspection.
- C. application level.
- D. circuit.

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

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

Scenario Questions

When writing this type of item, there are a number of considerations that must be kept in mind. 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
correct conclusions – do not force the candidate to make assumptions. The associated items should be in some sort of sequence and follow a logical progression. Also, 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.

**WHAT TO AVOID WHEN CONSTRUCTING ITEMS**

Following are examples of what to avoid when constructing quality items. Please note that these items will not appear on future exams.

Example 1

Stem: Which of the following methods of providing telecommunication continuity involves routing traffic through split or duplicate cable facilities?

Options:
- A. Diverse routing
- B. Alternative routing
- C. Redundancy
- D. Long haul network diversity

Key: A

Notice that a key word from the stem “routing” is in the answer. Avoid using important words in the stem and the answer or any of the distracters.

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 CISM 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.
ITEM DEVELOPMENT FORM

All items must be submitted on an Item Development Form (see Appendix B) and must be written in English. The Form includes:

- Name (Item Writer’s name)
- Domain/Task (Refer to Appendix A – CISM Job Practice Analysis)
- Knowledge Statement (Refer to Appendix A – CISM Job Practice Analysis)
- Item Stem
- Item Options
- Key (always have option “A” be the key for processing purposes)
- Justification (Reasons why the key is correct and the other three options are incorrect)
- Reference Source (Refer to KNET on the ISACA website at http://www.isaca.org/knet)

ITEM SUBMISSION AND REVIEW PROCESS

Each item submitted must include all fields listed on the Item Development Form. Please use Microsoft Word when submitting items. Multiple items should be included in one document. All items MUST be submitted in English. Submit completed forms to ISACA for initial review. These can be e-mailed to CISM@isaca.org, or mailed to the Exam Development Coordinator at ISACA headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, Illinois 60008 USA.

An initial review will be performed by the Exam Development Coordinator 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 you with appropriate and constructive feedback by the CISM TEC. In some cases an item will be judged to be in need of some revision and will be recommended for later resubmission after suggested changes are made. In other cases an item may be considered to be too flawed to be considered for rewrite and resubmission.

Items that pass the initial review will be forwarded for review and critique by the full membership of the CISM TEC. At this point your item(s) may again be accepted or returned for further work. If returned, the item will include appropriate and constructive feedback. If accepted, the item will become the property of ISACA and you will receive the appropriate payment and continuing credit hours for each item accepted.
Appendix A

CISM Job Practice Analysis

**Information Security Governance**: Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

**Tasks**

1.1 Develop the information security strategy in support of business strategy and direction.
1.2 Obtain senior management commitment and support for information security throughout the enterprise.
1.3 Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.
1.4 Establish reporting and communication channels that support information security governance activities.
1.5 Identify current and potential legal and regulatory issues affecting information security and access their impact on the enterprise.
1.6 Establish and maintain information security policies that support business goals and objectives.
1.7 Ensure the development of procedures and guidelines that support information security policies.
1.8 Develop business case and enterprise value analysis that support information security program(me) investments.

**Knowledge Statements**

1.1 Knowledge of information security concepts.
1.2 Knowledge of the relationship between information security and business operations.
1.3 Knowledge of techniques used to secure senior management commitment and support of information security management.
1.4 Knowledge of methods of integrating information security governance into the overall enterprise governance framework.
1.5 Knowledge of practices associated with an overall policy directive that captures senior management level direction and expectations for information security in laying the foundation for information security management within and organization.
1.6 Knowledge of an information security steering group function.
1.7 Knowledge of information security management roles, responsibilities, and organizational structure.
1.8 Knowledge of areas of governance: (for example, risk management, data classification management, network security, system access…).
1.9 Knowledge of centralized and decentralized approaches to coordinating information security.
1.10 Knowledge of legal and regulatory issues associated with Internet businesses, global transmissions and trans-border data flows (for example, privacy, tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security).
1.11 Knowledge of common insurance policies and imposed conditions: (for example, crime or fidelity insurance, business interruptions).
1.12 Knowledge of the requirements for the content and retention of business records and compliance.
1.13 Knowledge of the process for linking policies to enterprise business objectives.
1.14 Knowledge of the function and content of essential elements of an information security program(me) (for example, policy statements, procedures and guidelines).
1.15 Knowledge of techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures.
1.16 Knowledge of information security process improvement and its relationship to traditional process management.
1.17 Knowledge of information security process improvement and its relationship to security architecture development, and modeling.
1.18 Knowledge of information security process improvement and its relationship to security infrastructure.
1.19 Knowledge of generally accepted international standards for information security management and related process improvement models.
1.20 Knowledge of the key components of cost benefit analysis and enterprise transformation/migration plans: (for example: architectural alignment, organizational positioning, change management, benchmarking, market/competitive analysis).
1.21 Knowledge of methodology for business case development and computing enterprise value proposition.

**Risk Management:** Identify and manage information security risk to achieve business objectives.

*Tasks*

2.1 Develop a systematic, analytical, and continuous risk management process.
2.2 Ensure that risk identification, analysis, and mitigation activities are integrated into life cycle processes.
2.3 Apply risk identification and analysis methods.
2.4 Define strategies and prioritize options to mitigate risk to levels acceptable to the enterprise.
2.5 Report significant changes in risk to appropriate levels of management on both a periodic and event-driven basis.
Knowledge Statements

2.01 Knowledge of information resources used in support of business processes.
2.02 Knowledge of information resource valuation methodologies.
2.03 Knowledge of information classification.
2.04 Knowledge of the principles of development of baselines and their relationship to risk based assessments of control requirements.
2.05 Knowledge of life-cycle based risk management principles and practices.
2.06 Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity, and availability of information resources.
2.07 Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events.
2.08 Knowledge of use of gap analysis to assess generally accepted standards of good practice for information security management against current state.
2.09 Knowledge of recovery time objectives (RTO) for information resources and how to determine RTO.
2.10 Knowledge of RTO and how it relates to business continuity and contingency planning objectives and processes.
2.11 Knowledge of risk mitigation strategies used in defining security requirements for information resources supporting business applications.
2.12 Knowledge of cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
2.13 Knowledge of managing and reporting status of identified risks.

Information Security Program(me) Management: Design, develop and manage an information security program(me) to implement the information security governance framework.

Tasks

3.1 Create and maintain plans to implement the information security governance framework.
3.2 Develop information security baseline(s).
3.3 Develop procedures and guidelines to ensure business processes address information security risk.
3.4 Develop procedures and guidelines for IT infrastructure activities to ensure compliance with information security policies.
3.5 Integrate information security program(me) requirements into the organization’s life cycle activities.
3.6 Develop methods of meeting information security policy requirements that recognize impact on end-users.
3.7 Promote accountability by business process owners and other stakeholders in managing information security risks.
3.8 Establish metrics to manage the information security governance framework.
3.9 Ensure that internal and external resources for information security are identified, appropriated and managed.

Knowledge Statements

3.01 Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analyses.
3.02 Knowledge of project management methods and techniques.
3.03 Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise.
3.04 Knowledge of security baselines and configuration management in the design and management of business applications and the infrastructure.
3.05 Knowledge of information security architectures: (for example, single sign-on, rules-based as opposed to list-based system access control for systems, limited points of systems administration).
3.06 Knowledge of information security technologies, for example, cryptographic techniques and digital signatures, to enable management to select appropriate controls.
3.07 Knowledge of security procedures and guidelines for business processes and infrastructure activities.
3.08 Knowledge of the systems development life cycle methodologies (for example traditional SDLC, prototyping).
3.09 Knowledge of planning, conducting, reporting, and follow-up of security testing.
3.10 Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise’s information security governance framework.
3.11 Knowledge of the relative benefits and costs of physical, administrative and technical controls.
3.12 Knowledge of planning, designing, developing, testing, and implementing information security requirements into an enterprise’s business processes.
3.13 Knowledge of security metrics design, development and implementation.
3.14 Knowledge of acquisition management methods and techniques: (for example, evaluation of vendor service level agreements, preparation of contracts).

Information Security Management: Oversee and direct information security activities to execute the information security program(me).

Tasks

4.1 Ensure that the rules of use for information systems comply with the enterprise’s information security policies.
4.2 Ensure that the administrative procedures for information systems comply with the enterprise’s information security policies.
4.3 Ensure that services provided by other enterprises including outsourced providers are consistent with established information security policies.
4.4 Use metrics to measure, monitor, and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
4.5 Ensure that information security is not compromised throughout the change management process.
4.6 Ensure that vulnerability assessments are performed to evaluate effectiveness of existing controls.
4.7 Ensure that non-compliance issues and other variances are resolved in a timely manner.
4.8 Ensure the development and delivery of the activities that can influence culture and behaviour of staff including information security education and awareness.

Knowledge Statements

4.01 Knowledge of how to interpret information security policies into operational use.
4.02 Knowledge of information security administration process and procedures.
4.03 Knowledge of methods for managing the implementation of the enterprise’s information security program(me) through third parties including trading partners and security services providers.
4.04 Knowledge of continuous monitoring of security activities in the enterprise’s infrastructure and business applications.
4.05 Knowledge of methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators.
4.06 Knowledge of change and configuration management activities.
4.07 Knowledge of information security management due diligence activities and reviews of the infrastructure.
4.08 Knowledge of liaison activities with internal/external assurance providers performing information security reviews.
4.09 Knowledge of due diligence activities, reviews, and related standards for managing and controlling access to information resources.
4.10 Knowledge of external vulnerability reporting sources, that provide information which may require changes to the information security in applications and infrastructure.
4.11 Knowledge of events affecting security baselines that may require risk re-assessments and changes to information security requirements in security plans, test plans and re-performance.
4.12 Knowledge of information security problem management practices
4.13 Knowledge of information security manager facilitative roles as change agents, educators, and consultants.
4.14 Knowledge of the ways in which culture and cultural differences affect the behaviour of staff.
4.15 Knowledge of the activities that can change culture and behaviour of staff.
4.16 Knowledge of methods and techniques for security awareness training and education.

Response Management: Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

Tasks

5.1 Develop and implement processes for detecting, identifying and analyzing security related events.
5.2 Develop response and recovery plans including organizing, training, and equipping the teams.
5.3 Ensure periodic testing of the response and recovery plans where appropriate.
5.4 Ensure the execution of response and recovery plans as required.
5.5 Establish procedures for documenting an event as a basis for subsequent action including forensics when necessary.
5.6 Manage post event reviews to identify causes and corrective actions.

Knowledge Statements

5.01 Knowledge of the components of an incident response capability.
5.02 Knowledge of information security emergency management practices (for example, production change control activities, development of computer emergency response team).
5.03 Knowledge of disaster recovery planning and business recovery processes.
5.04 Knowledge of disaster recovery testing for infrastructure and critical business applications.
5.05 Knowledge of escalation process for effective security management.
5.06 Knowledge of intrusion detection policies and processes.
5.07 Knowledge of help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with the help desks.
5.08 Knowledge of the notification process in managing security incidents and recovery: (for example, automated notice and recovery mechanisms for example in response to virus alerts in a real-time fashion).
5.09 Knowledge of the requirements for collecting and presenting evidence; rules for evidence, admissibility of evidence, quality and completeness of evidence.
5.10 Knowledge of post incident reviews and follow-up procedures.
Appendix B

Item Development Form

Sample Question using the Item Development Form

Name: Joe Smith

Domain/Task: 0302
Knowledge Statement: 0317

Item Stem:

Item Options:
A. Key
B. Distracter
C. Distracter
D. Distracter

Key: A

Justification:
A. Why “A” is the only correct answer
B. Why this distracter is incorrect
C. Why this distracter is incorrect
D. Why this distracter is incorrect

Reference Source: Refer to KNET on ISACA’s website for a listing of applicable reference materials. http://www.isaca.org/knet
**CISM ITEM DEVELOPMENT GUIDE**

Appendix C

**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 an information security **management** concept at the appropriate experience level of the test candidate (3 – 5 years information security management experience)?

2. Does the item test only one information security **management** concept?

3. Is your item clear?

4. Is there enough information (scenario) 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 answer to your stem for any situation, organization or culture? Many items are returned because there may be a situation when there is more than one possible keys 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 information security procedures…?” All options must be information security procedures.

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

8. Have you avoided having words or phrases in the key that appear in the stem?

9. Have you avoided unnecessary text or jargon from the stem or options?

10. Have you avoided using subjective terms such as “frequently”, “often”, “common”…. in the stem and options?

11. Have you avoided using absolute terms such as “all”, “never”, “always”… in the stem and options?

12. Have you avoided asking a negative question – using such terms as “least”, “not”, “except”…?