CISM® ITEM DEVELOPMENT GUIDE

Updated March 2017

ISACA
Trust in, and value from, information systems

CISM ITEM DEVELOPMENT GUIDE

TABLE OF CONTENTS

CISM ITEM DEVELOPMENT GUIDE

PURPOSE OF THE CISM ITEM DEVELOPMENT GUIDE

The purpose of the CISM Item Development Guide (Guide) is to provide assistance to item writers in their efforts to increase the quality of new items for the CISM exam. 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 the Guide, please pay particular attention to the item writing principles. Applying these principles will greatly enhance the chances of your items being accepted.

CISM EXAM STRUCTURE

ISACA and the CISM Certification Committee periodically perform a CISM 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 CISM exam. Questions must be written to test a candidate's knowledge of established process and content areas defined by the CISM Job Practice Analysis.

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 might not reflect the more global position or circumstance. Since the exam and CISM items are developed for the international information security community, this will require the item writer to be flexible when determining a globally accepted practice.

CISM ITEM DEVELOPMENT GUIDE

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 alternatives.

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 Choices (Alternatives):
The alternatives complete the introductory statement or answer the question and consist of one correct answer (key) and three incorrect answers or distractors.

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

Distractors:
Distractors are the incorrect alternatives 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 CISM 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 "CISM 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 distractors. The distractors should not be made up words or phrases. Distractors should appear to be correct alternatives to an inexperienced professional. The development of quality distractors is usually the most difficult task for an item writer. If you have difficulty with this part of item development, consult with your colleagues. Also think about what an inexperienced IT professional might think the correct answer would be. These incorrect experiences make for the best distractors.

STEP 4 Include a thorough explanation of why the keyable answer is correct as well as why each distractor is not a correct alternative. It is not acceptable to simply state that the distractors 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 (using such words as NOT, LEAST, EXCEPT, etc. in the stem) 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, "CISM Job Practice."
3. Ensure that the stem and all alternatives are compatible with each other. For example, if your stem reads, "Which of the following controls will BEST…," then all alternatives must be controls.
4. Keep the stem and alternatives as short as possible by avoiding the use of unnecessary text or jargon. Do not attempt to teach the candidate a concept or theory by providing too much information before asking the question. Remember, this is an exam, not a classroom.
5. Include common words or phrases in the item stem rather than in the key and distractors.
6. Write all alternatives the same approximate length and format. A good test taker with very little knowledge or experience in IT will select the alternative that is either the shortest or the longest in length and will most likely choose the correct answer.
7. Write alternatives that are grammatically consistent with the item stem and maintain a parallel grammatical format. For example if the key begins with a verb ending with "ing," then all distractors must begin with a verb ending with "ing."
8. Use only professionally acceptable or technical terminology in the item stem and alternatives.

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 these types of clues to 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 alternative 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, making it easier for candidates to eliminate distractors.
4. Terms such as "least," "not," or "except" are negative and require a candidate to choose an incorrect or least preferred alternative, rather than a correct or preferred alternative. 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 alternative, or including portions of one alternative in another. These are considered to be "multiple, multiple alternatives" and do not test well. Each alternative should stand on its own.
7. Items with alternatives "all of the above" or "none of the above" will be returned to the item writer. Good test takers know that these types of alternatives are very rarely correct and do not make good distractors.
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 writing "True/False" questions such as "Which of the following are true?"
11. 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 CISM exam is administered globally and across all industries. The concepts tested must be accepted and recognized practice world-wide and in all industries.

ITEM EXAMPLES

Items can either be direct question or incomplete statements and are described below. These questions were developed as sample items for item writing training and do not appear on any exams.

Direct question:

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

Alternatives:
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:

Alternatives:

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 start with a lowercase word and are followed by a period, as each response serves to complete the sentence started in the stem.

WHAT TO AVOID WHEN CONSTRUCTING ITEMS

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

Example 1:

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

Alternatives:

A. Prevents any 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

Notice that a key word from the stem ("prevention") leads to the word "prevent" in the answer. Avoid using important similar words in the stem and the answer as this makes the key very obvious. Also, absolute words are used in alternatives B (all) and C (constantly), making them easily eliminated. Avoid using absolute or subjective terms in the alternatives.

Example 2:

Stem: Which of the following is **MOST** important to writing good information security policies?

Alternatives:

A. Ensure that they are easy to read and understand
B. Ensure that they allow for flexible interpretation
C. Ensure that they describe technical vulnerability
D. Ensure that they change whenever operating systems are upgraded

Key: A

Notice that the first three words are repeated in each item. This question can be easily rewritten to make it a more concise item. Simply include the three words at the end of the stem as follows:

New Stem: Which of the following is **MOST** important to writing good information security policies? Ensure the policies:

New Alternatives:

A. are easy to read and understand.
B. allow for flexible interpretation.
C. describe technical vulnerability.
D. change whenever operating systems are upgraded.

The stem becomes an incomplete sentence with the alternatives completing the sentence.

Example 3:

Stem: When building support for an information security program, which of the following should be performed **FIRST**?

Alternatives:

A. Identification of existing vulnerabilities
B. Cost-benefit analysis
C. Business impact analysis
D. Formal risk assessment

Key: A

This item is an example of a timing question and introduces subjectivity. Both alternatives C and D could be the correct answer depending on the situation within a given organization. Testing what is to be done FIRST does not test well unless there is a definite FIRST step in a process. However, when there is a definite FIRST step, the question often becomes too easy.

Example 4:

Stem: Security awareness programs should be:

Alternatives:

A. standardized throughout the organization.
B. customized depending on the target audiences.
C. avoided since key security vulnerabilities may be disclosed.
D. limited to IS personnel.

Key: A

Example 4 is another instance of a subjective item. In some organizations, security awareness programs are mandated to be standardized while in others, they prefer programs to be customized. The answer depends on the organization's security needs and program.

When writing questions on areas that tend to be subjective in nature, such as what makes for a good information security awareness program, or testing roles and responsibilities, be very careful to ensure that there is only one correct answer in all situations. If you are not sure the answer will apply to all situations, then add more content to the stem to take away the subjectivity. For example, you could describe an organization's structure so that it is clear to an experienced information security manager what type of security awareness program would perform best.

Example 5:

Stem: Record retention policies generally are driven by:

Alternatives:

A. legal and regulatory requirements.
B. risk levels acceptable to the organization.
C. business goals and objectives.
D. audit and assurance requirements.

Key: A

This question illustrates the effect of having weak distractors or too obvious of an answer. Answers like legal/regulatory requirements make for poor questions because there are no other strong alternatives to distract candidates away from the correct alternative.

The previous examples represent the most common reasons why items are <u>not</u> accepted. Other reasons why an item may be returned include the item is too technical or definitional. When writing items of a technical nature, remember, the content needs to test the knowledge of an experienced information security MANAGER, not a technician. Also remember that the CISM

exam is a practical examination testing an individual's application of information security management knowledge. If an item is returned as too definitional, it usually means that the item is simply asking the candidate whether they know the definition of a technology or security terminology as opposed to how to apply the knowledge or concept.

CISM JOB PRACTICE – WHAT IS IT?

The CISM Job Practice lists the relevant tasks performed by IT professionals working in the areas of security, risk and control and the knowledge necessary to perform those tasks. These tasks and knowledge will be the basis for CISM exam questions. The goal of the CISM exam is to present experience-based questions testing knowledge necessary to perform a task. The CISM 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 CISM 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—CISM JOB PRACTICE when rubricing an item. ***In the online submission form, rubrics are referred to as "Classifications." Task statements are "Primary Classifications" and knowledge statements are "Secondary Classifications."***

ITEM SUBMISSION AND REVIEW PROCESS

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

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

An initial review will be performed by an ISACA representative to ensure completeness and compliance with the item writing principles. Items that are judged to be flawed in any significant way will be sent back to the item writer with appropriate and constructive feedback. Items accepted by the ISACA representative will be forwarded to the CISM Exam Item Development Working Group (EIDWG) to be considered for inclusion in the exam item pool.

Once reviewed by the EIDWG, the item will be accepted or returned. If returned by the EIDWG, the item will be returned to the writer, including appropriate and constructive feedback. If accepted, the item will become the property of ISACA and the item writer will receive

honorarium payment along with 2 CPE credit hours. An honorarium of US $50.00 will be awarded for each item accepted.

Appendix A

CISM Job Practice – Effective 2017

To assist with the assigning of a rubric to an item, the knowledge statements listed in this Job Practice are mapped to corresponding task statements. At the end of each knowledge statement, the task statements which best apply are listed. A given knowledge statement may map to more than one task statement and the focus of the knowledge (testing concept) should be different based upon the specific task for which it is written.

Domain 1—Information Security Governance: Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives.

Task Statements:

1.1 Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

1.2 Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.

1.4 Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

1.5 Develop business cases to support investments in information security.

1.6 Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.

1.7 Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

1.8 Define, communicate, and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.

1.9 Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

Knowledge Statements:

k1.1 Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research) (Task: 1.1.1)

k1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices (Tasks: 1.1.1, 1.1.3, 1.1.4, 1.1.6)

k1.3 Knowledge of available information security governance frameworks (Tasks: 1.1.2, 1.1.3)

k1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development (Tasks: 1.1.1, 1.1.2, 1.1.3)

k1.5 Knowledge of the fundamental concepts of governance and how they relate to information security (Tasks: 1.1.2, 1.1.3)

k1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework (Tasks: 1.1.2, 1.1.3)

k1.7 Knowledge of methods to integrate information security governance into corporate governance (Tasks: 1.1.3, 1.1.6)

k1.8 Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development (Task: 1.1.4)

k1.9 Knowledge of content in, and techniques to develop, business cases (Task: 1.1.5)

k1.10 Knowledge of strategic budgetary planning and reporting methods (Tasks: 1.1.1, 1.1.5, 1.1.9)

k1.11 Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy (Tasks: 1.1.1, 1.1.6)

k1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact) (Tasks: 1.1.1, 1.1.5, 1.1.7)

k1.13 Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security) (Task: 1.1.7)

k1.14 Knowledge of roles and responsibilities of the information security manager (Task: 1.1.8)

k1.15 Knowledge of organizational structures, lines of authority and escalation points (Task: 1.1.8)

k1.16 Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users) (Task: 1.1.8)

k1.17 Knowledge of processes to monitor performance of information security responsibilities (Task: 1.1.8)

k1.18 Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization (Task: 1.1.8)

k1.19 Knowledge of methods to select, implement and interpret key information security metrics (e.g. key performance indicators [KPIs] or key risk indicators [KRIs]) (Task: 1.1.9)

Domain 2—Information Risk Management: Manage information risk to an acceptable level based on risk appetite in order to meet organizational goals and objectives.

Task Statements:

2.1 Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
2.2 Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
2.3 Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.
2.4 Identify, recommend or implement appropriate risk treatment/response alternatives to manage risk to acceptable levels based on organizational risk appetite.
2.5 Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
2.6 Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization.
2.7 Monitor for internal and external factors (e.g., key risk indicators [KRIs], threat landscape, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.
2.8 Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.
2.9 Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

Knowledge Statements:

k2.1 Knowledge of methods to establish an information asset classification model consistent with business objectives (Tasks: 1.2.1, 1.2.2)
k2.2 Knowledge of considerations for assigning ownership of information assets and risk (Task: 1.2.1)
k2.3 Knowledge of methods to identify and evaluate the impact of internal or external events on information assets and the business (Tasks: 1.2.1, 1.2.7)
k2.4 Knowledge of methods used to monitor internal or external risk factors (Tasks: 1.2.2, 1.2.7)
k2.5 Knowledge of information asset valuation methodologies (Task: 1.2.1)
k2.6 Knowledge of legal, regulatory, organizational and other requirements related to information security (Tasks: 1.2.2, 1.2.7, 1.2.8)

k2.7 Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities (Tasks: 1.2.1, 1.2.3, 1.2.7, 1.2.8)
k2.8 Knowledge of events that may require risk reassessments and changes to information security program elements (Tasks: 1.2.1, 1.2.3, 1.2.7, 1.2.8)
k2.9 Knowledge of information threats, vulnerabilities and exposures and their evolving nature (Tasks: 1.2.3, 1.2.7)
k2.10 Knowledge of risk assessment and analysis methodologies (Tasks: 1.2.3, 1.2.4, 1.2.7)
k2.11 Knowledge of methods used to prioritize risk scenarios and risk treatment/response alternatives (Tasks: 1.2.4, 1.2.5, 1.2.7)
k2.12 Knowledge of risk reporting requirements (e.g., frequency, audience, content) (Tasks: 1.2.5, 1.2.8, 1.2.9)
k2.13 Knowledge of risk treatment/response alternatives (avoid, mitigate, accept or transfer) and methods to apply them (Tasks: 1.2.4, 1.2.5, 1.2.7)
k2.14 Knowledge of control baselines and standards and their relationships to risk assessments (Tasks: 1.2.3, 1.2.5)
k2.15 Knowledge of information security controls and the methods to analyze their effectiveness (Task: 1.2.4)
k2.16 Knowledge of gap analysis techniques as related to information security (Tasks: 1.2.3, 1.2.5)
k2.17 Knowledge of techniques for integrating information security risk management into business and IT processes (Tasks: 1.2.5, 1.2.6)
k2.18 Knowledge of compliance reporting requirements and processes (Tasks: 1.2.6, 1.2.8, 1.2.9)
k2.19 Knowledge of cost/benefit analysis to assess risk treatment alternatives (Tasks: 1.2.4, 1.2.5)

Domain 3—Information Security Program Development and Management: Develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture.

Task Statements:

3.1 Establish and/or maintain the information security program in alignment with the information security strategy.
3.2 Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.
3.3 Identify, acquire and manage requirements for internal and external resources to execute the information security program.
3.4 Establish and maintain information security processes and resources (including people and technologies) to execute the information security program in alignment with the organization's business goals.

3.5 Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

3.6 Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

3.7 Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system development, business continuity, disaster recovery) to maintain the organization's security strategy.

3.8 Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) and monitor adherence to established requirements in order to maintain the organization's security strategy.

3.9 Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

3.10 Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

Knowledge Statements:

k3.1 Knowledge of methods to align information security program requirements with those of other business functions (Tasks: 1.3.1, 1.3.2)

k3.2 Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources (Tasks: 1.3.1, 1.3.3, 1.3.4)

k3.3 Knowledge of current and emerging information security technologies and underlying concepts (Tasks: 1.3.3, 1.3.4)

k3.4 Knowledge of methods to design and implement information security controls (Tasks: 1.3.7, 1.3.8)

k3.5 Knowledge of information security processes and resources (including people and technologies) in alignment with the organization's business goals and methods to apply them (Tasks: 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7)

k3.6 Knowledge of methods to develop information security standards, procedures and guidelines (Task: 1.3.5)

k3.7 Knowledge of internationally recognized regulations, standards, frameworks and best practices related to information security program development and management (Tasks: 1.3.7, 1.3.7, 1.3.8)

k3.8 Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines (Tasks: 1.3.5, 1.3.6)

k3.9 Knowledge of training, certifications and skill set development for information security personnel (Task: 1.3.6)

k3.10 Knowledge of methods to establish and maintain effective information security awareness and training programs (Tasks: 1.3.5, 1.3.7)

k3.11 Knowledge of methods to integrate information security requirements into organizational processes (e.g., access management, change management, audit processes) (Tasks: 1.3.1, 1.3.2, 1.3.3, 1.3.7)

k3.12 Knowledge of methods to incorporate information security requirements into contracts, agreements and third-party management processes (Tasks: 1.3.2, 1.3.3, 1.3.8)
k3.13 Knowledge of methods to monitor and review contracts and agreements with third parties and associated change processes as required (Task: 1.3.3)
k3.14 Knowledge of methods to design, implement and report operational information security metrics (Tasks: 1.3.3, 1.3.9, 1.3.10)
k3.15 Knowledge of methods for testing the effectiveness and efficiency of information security controls (Tasks: 1.3.9, 1.3.10)
k3.16 Knowledge of techniques to communicate information security program status to key stakeholders (Tasks: 1.3.6, 1.3.10)

Domain 4—Information Security Incident Management: Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

Task Statements:

4.1 Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.
4.2 Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
4.3 Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.
4.4 Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.
4.5 Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.
4.6 Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.
4.7 Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.
4.8 Establish and maintain communication plans and processes to manage communication with internal and external entities.
4.9 Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
4.10 Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.

Knowledge Statements

- k4.1 Knowledge of incident management concepts and practices (Tasks: 1.4.1, 1.4.4)
- k4.2 Knowledge of the components of an incident response plan (Tasks: 1.4.1, 1.4.2, 1.4.3, 1.4.10)
- k4.3 Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan (Tasks: 1.4.1, 1.4.2, 1.4.4, 1.4.10)
- k4.4 Knowledge of incident classification/categorization methods (Tasks: 1.4.1, 1.4.2, 1.4.3, 1.4.4)
- k4.5 Knowledge of incident containment methods to minimize adverse operational impact (Tasks: 1.4.1, 1.4.2)
- k4.6 Knowledge of notification and escalation processes (Tasks: 1.4.1, 1.4.2, 1.4.5, 1.4.8)
- k4.7 Knowledge of the roles and responsibilities in identifying and managing information security incidents (Tasks: 1.4.2, 1.4.3, 1.4.5, 1.4.6, 1.4.7, 1.4.8)
- k4.8 Knowledge of the types and sources of training, tools and equipment required to adequately equip incident response teams (Tasks: 1.4.4, 1.4.6)
- k4.9 Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody) (Tasks: 1.4.2, 1.4.4, 1.4.6)
- k4.10 Knowledge of internal and external incident reporting requirements and procedures (Tasks: 1.4.2, 1.4.8, 1.4.9)
- k4.11 Knowledge of postincident review practices and investigative methods to identify root causes and determine corrective actions (Tasks: 1.4.4, 1.4.7, 1.4.9)
- k4.12 Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents (Task: 1.4.9)
- k4.13 Knowledge of technologies and processes to detect, log, analyze and document information security events (Tasks: 1.4.3, 1.4.4)
- k4.14 Knowledge of internal and external resources available to investigate information security incidents (Tasks: 1.4.4, 1.4.5, 1.4.6)
- k4.15 Knowledge of methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process (Task: 1.4.4)
- k4.16 Knowledge of techniques to test the incident response plan (Tasks: 1.4.1, 1.4.6, 1.4.7)
- k4.17 Knowledge of applicable regulatory, legal and organization requirements (Tasks: 1.4.4, 1.4.9)
- k4.18 Knowledge of key indicators/metrics to evaluate the effectiveness of the incident response plan (Tasks: 1.4.4, 1.4.7, 1.4.9)

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

2. Does the item test only one CISM 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 distractor 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 alternatives compatible with each other? For example: "Which of the following controls…?" All alternatives must be controls.

7. Does the item have plausible distractors 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," "common" … in the stem and alternatives?

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

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