CISA®
Certified Information
Systems Auditor®
An ISACA® Certification

CISA® ITEM DEVELOPMENT GUIDE

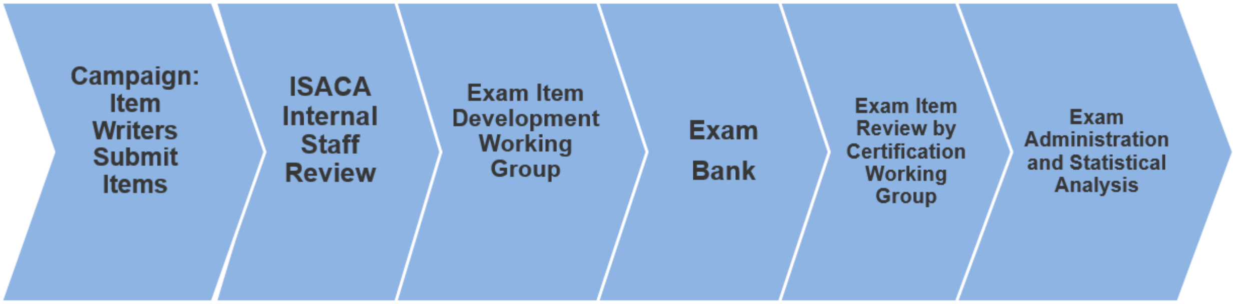
Updated October 2018

PURPOSE OF THE CISA ITEM DEVELOPMENT GUIDE

The purpose of the CISA Item Development Guide is to assist item writers in their efforts to write new items for the CISA exam. This guide is intended to familiarize writers with the item development process and give them tools and insights to help them create new items that will enhance the quality of the exam.

As you read through this Guide, please pay particular attention to the item writing principles. Applying these principles will greatly increase the chances of your items being accepted for the CISA exam.

THE CISA ITEM WRITING AND REVIEW PROCESS: AN OVERVIEW


Campaign: Item Writers Submit Items
ISACA Internal Staff Review
Exam Item Development Working Group
Exam Bank
Exam Item Review by Certification Working Group
Exam Administration and Statistical Analysis

ISACA conducts multiple item writing campaigns each year to generate new items for the CISA exam bank. You will receive an invitation to the campaign from our online item writing system, along with instructions for how to use the system to create and submit new items for review. Resources and guidance will also be available throughout each campaign to assist you.

Once you have submitted a new item, a member of the ISACA item development team will review the item for adherence to ISACA's item writing guidelines. ISACA staff reviewers are not subject matter experts, however; they are exam development experts and understand the types of questions that test well or poorly. While the ISACA staff review typically does not focus on the content of the item, they may provide suggestions for alternate wording to enhance the clarity of the text. Items that need revision to meet ISACA's guidelines are returned to the writer with feedback and can be resubmitted at any time before the campaign's final deadline.

Once ISACA staff determine that an item is ready to move forward, the item will then be included for review by the CISA Exam and Item Development Working Group (EIDWG), which is a panel of CISA subject matter experts from a variety of industries and regions. The working group meets a few weeks after the conclusion of the campaign to review the items with a focus on the content being tested. Items accepted by the working group go directly into ISACA's exam banks, and the item writer is paid an honorarium and awarded CPEs for each item accepted.

Items rejected by the working group are returned to the writer after the meeting with detailed feedback from the group.

While initial feedback from ISACA staff takes place on an ongoing basis during the campaign, final results from the EIDWG are typically available the week following the working group meeting. This means that once a campaign closes, feedback from the working group will not be available for approximately 4-6 weeks, depending on the meeting date.

TRAINING FOR NEW WRITERS

All new item writers are required to complete the online training program before participating in a regular CISA campaign. Writers enrolled in a training program are assigned to a member of the ISACA item development team, who will provide detailed feedback on submissions to help writers become familiar with the process and principles behind effective CISA item writing. Upon completing the training program, writers become eligible to participate in our regular CISA item writing campaigns.

WRITING QUALITY ITEMS

ISACA and the CISA Certification Working Group periodically perform a CISA Job Practice Analysis study to determine the tasks and knowledge currently required of IS audit professionals. The results of this analysis serve as the blueprint for the CISA exam and the CISA review materials. Exam questions must be written to test a candidate's knowledge of established process and content areas defined by the CISA Job Practice. Each new item accepted for the CISA bank must be assigned by the writer to a topic and a supporting task from the Job Practice, which is included at the end of this Guide.

When writing CISA items, it is necessary to consider the exam's target audience, which is the minimally competent CISA candidate. Items must be developed at the proper level of experience expected of the individual just passing the CISA exam, with three (3) to five (5) years of experience in auditing, controlling, monitoring and assessing information technology and business systems.

Item writers must also keep in mind that because the CISA exam is administered globally, the content and wording of items need to be applicable to and recognized by the international IS audit and control community.

ITEM FORMATS

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 alternatives.

> ***Item Stem:***
> The item stem contains the introductory statement to be completed or question to be answered. The stem often includes context describing a situation or circumstance related to the knowledge being assessed. Stems are usually written as direct questions, though sometimes stems are written as incomplete sentences to improve readability.
>
> ***Item Choices (Alternatives):***
> The alternatives complete the introductory statement or answer the question and consist of one correct answer (key) and three incorrect answers (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 against the others provided.
>
> ***Distractors:***
> Distractors are the incorrect alternatives, and writing effective distractors is one of the most challenging aspects of item writing. Distractors must clearly be not the best answer available, but they must appear to be plausible or possible answers to candidates who are not knowledgeable enough to choose the key.

As mentioned above, the majority of CISA exam items use a direct question format, as in the following example. (Please note that items in this Guide are not actual exam items.)

Stem: Which of the following concerns would **BEST** be addressed by the comparison of production application systems source code with an archive copy?

Alternatives:

A. File maintenance errors
B. Unauthorized modifications
C. Software version currency
D. Documentation discrepancies

Sometimes an incomplete statement is used in the stem, which looks like this:

Stem: The comparison of production application systems source code with an archive copy would **BEST** address:

Alternatives:

A. file maintenance errors.
B. unauthorized modifications.
C. software version currency.
D. documentation discrepancies.

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

ITEM TYPES TO AVOID

Items with the following issues will be returned to the item writer for revision by ISACA staff:

1. Items that ask a negatively phrased question – that is, asking which alternative does NOT apply, or which alternative is LEAST preferred. Negative questions require candidates to reverse their traditional mode of thinking and thus tend to test less well statistically.
2. Items that ask a true/false question or ask which of the alternatives is a true statement.
3. Items with alternatives in a "multiple-multiple" format – that is, components of some alternatives are contained within others. It is permissible to use lists in answer choices, but no element contained in one choice should be repeated in any other choice.
4. Items with alternatives such as "all of the above", "none of the above" or "Both B and C". Each alternative must be able to stand alone. (Along these lines, alternatives such as "take no action" or "ignore this issue" are usually too close to "none of the above." Such alternatives make poor distractors and should also be avoided.)
5. Items that use a fill-in-the-blank format.
6. Items that test knowledge of vendor-specific products or region-specific regulations.
7. Items that directly test knowledge of the meanings of terminology. Remember that the CISA exam is an experience-based exam - a definitional question can be answered by an otherwise inexperienced candidate who happens to have studied a review manual or other reference, and so such questions do not require candidates to rely on their professional experience to answer correctly.

STEPS TO WRITING ITEMS

STEP 1 Select a topic from the CISA Job Practice for your new item. Items should be written to test knowledge necessary to perform a specific task, and they should focus on a single topic rather than trying to test multiple concepts at once. Refer to the CISA Job Practice at the end of this Guide for a list of the available topics and supporting tasks.

STEP 2 Write the item stem and key (correct answer). **When submitting items, you should always make choice A the correct answer.**

STEP 3 Develop plausible distractors. Distractors should not be made-up words or phrases, and they should appear to be correct alternatives to an inexperienced professional. It may help when creating distractors to consider what an inexperienced IT professional might think the correct answer would be, or to ask colleagues what sorts of mistakes they can imagine an inexperienced professional making.

STEP 4 In the space provided for rationales, include a thorough explanation of why the key is correct, as well as why each distractor is not a correct alternative. This helps ISACA reviewers and the working group understand your intended testing concept.

STEP 5 Include any reference sources that support your item. Submitted items must include at least one reference. Any reputable reference is acceptable, as long as it teaches best practice and supports your answer. Check out www.isaca.org/knowledge_center for some applicable references.

STEP 6 Review the item using the Item Writing Checklist.

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

GOOD PRACTICES FOR ITEM WRITING

1. Ensure the item is testing only one concept and reflects the chosen topic and supporting task statements. Items that attempt to test multiple concepts at once are typically returned for being unclear or potentially confusing.
2. Ensure the item is appropriate for a CISA candidate with three to five years of experience – not too fundamental or easy, not too advanced or difficult.
3. Ensure the stem and alternatives are concise and do not contain unnecessary detail or explanation. Keep in mind that a candidate has only a short time to read, understand and answer each question on the exam.
4. Ensure the item is not “teaching” the candidate – that is, explaining a concept explicitly within the stem or alternatives.

5. Ensure the key would always be the correct or best available answer for the situation presented in the stem. Items are often returned because they do not provide enough context for a candidate to arrive at the correct answer without making assumptions, or because the correct answer could vary depending on the organization or its circumstances.
6. If the item is testing roles and responsibilities, ensure the correct answer is not dependent on the organization's size, structure or other organization-specific factors.
7. Ensure the wording of the item does not introduce subjectivity – words such as "commonly", "frequently" or "rarely" are dependent on interpretation and should almost always be avoided.
8. Ensure that absolute words such as "all", "always" or "never" are not used – it is often too easy for candidates to rule out distractors with this wording.
9. Ensure that personal or gender pronouns (you, your, she, he, her, his, etc.) are avoided, as well as ad hoc organization names such as "Company XYZ".
10. If an important word appears in both the stem and the key, it should appear in at least one distractor as well, so that the candidate is not inadvertently given a clue to the correct answer.
11. Ensure the alternatives are compatible with the stem. For example, if the question begins with "Which of the following controls…," all the alternatives should be controls.
12. Ensure that any terminology or practice referred to in the item is globally familiar and in current use.
13. Ensure the alternatives do not introduce new information that is not apparent from the stem. Candidates should be able to begin formulating an answer even before viewing the alternatives.
14. Ensure all alternatives are roughly the same length and are constructed similarly. For example, if the key starts with a verb ending in "ing", the distractors should also start that way. This keeps certain alternatives from standing out unnecessarily.

ITEM WRITING CHECKLIST

1. Does the item have any issues listed in the Item Types to Avoid section? If so, those issues must be addressed prior to submission.
2. Does the item adhere to the item writing guidelines presented in the Good Practices for Item Writing section?
3. Has the item been checked for grammar and spelling, and is it easily understood on first reading? Remember that the candidate does not get to see the rationales for the stem and alternatives during the exam, so if one has to read the rationales to understand the item, it probably needs clarification.
4. Have a topic and supporting task for the item been selected, and does the item's testing concept align with them?
5. Have rationales been included for the stem and alternatives?
6. Has at least one reference been provided for the item?

EXAMPLE ITEMS

Now, let's take a look at some examples of potential issues you may encounter when constructing items.

Example 1:

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

Alternatives:

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
There is not enough information in the stem to be able to choose only one correct answer. An IS auditor might have good reason to look at any or all of these things when reviewing a disaster recovery plan. It is sometimes possible to fix this type of issue by adding a qualifier such as "BEST" or "MOST important" to the question, but in this case, without more context, it would be difficult to say for sure which of the alternatives is most important for the auditor to review – it depends on the organization and situation. This item would be returned, because as written it is too subjective.

Example 2:

Stem: An IS auditor learns that a manager in the loan department of a financial institution changes the interest rates of several loans in the financial system. Which of the following is the auditor's **BEST** recommendation to address this situation?

Alternatives:

A. Functional access controls should be strengthened.
B. Changes to loan information should be logged.
C. Senior management should supervise changes to loan information.
D. Change management controls should be implemented.

Key: A
In this item, the issue is that the stem assumes functional responsibility. It is not clear from the stem that the manager is doing anything wrong by making these changes – it is possible that in some organizations, a manager would have this type of access. Practices related to roles and responsibilities can vary in different geographic regions as well. While it is possible to write effective items that test roles and responsibilities, great care must be taken to

ensure the test taker has enough context to choose one best answer that would apply to any organization.

Example 3:

Stem: An organization uses spreadsheets to calculate project cost estimates, and totals for each cost category are then keyed into the job costing system. Which of the following is the BEST control to ensure the accuracy of data entered into the job costing system?

Alternatives:

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
This item lacks specific IS audit context. While there are certain financial concerns that an IS auditor might need to be aware of, the alignment of this item with the CISA body of knowledge and job practice is not strong enough, making it unlikely that the item would eventually be accepted for the CISA exam. It is often possible to revise items to strengthen the audit focus, and one good way to do that is to reframe the question from the auditor's perspective: What would be best or most important to review or recommend in the given situation?

NOTE: The new CISA Job Practice will not be in effect until June 2019. It is included in this guide to ensure new item submissions are mapped to the new content.

Trust in, and value from, information systems

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 1: Information System Auditing Process	
A.	**Planning**
1A1.	IS Audit Standards, Guidelines, and Codes of Ethics
1A2.	Business Processes
1A3.	Types of Controls
1A4.	Risk-Based Audit Planning
1A5.	Types of Audits and Assessments
B.	**Execution Subtopics**
1B1.	Audit Project Management
1B2.	Sampling Methodology
1B3.	Audit Evidence Collection Techniques
1B4.	Data Analytics
1B5.	Reporting and Communication Techniques
1B6.	Quality Assurance and Improvement of Audit Process
Content Area 2: Governance and Management of IT	
A.	**IT Governance Subtopics**
2A1.	IT Governance and IT Strategy
2A2.	IT-Related Frameworks
2A3.	IT Standards, Policies, and Procedures
2A4.	Organizational Structure
2A5.	Enterprise Architecture
2A6.	Enterprise Risk Management
2A7.	Maturity Models
2A8.	Laws, Regulations, and Industry Standards affecting the Organization
B.	**IT Management**
2B1.	IT Resource Management
2B2.	IT Service Provider Acquisition and Management
2B3.	IT Performance Monitoring and Reporting
2B4.	Quality Assurance and Quality Management of IT

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 3: Information Systems Acquisition, Development, and Implementation

A. Information Systems Acquisition and Development

- 3A1. Project Governance and Management
- 3A2. Business Case and Feasibility Analysis
- 3A3. System Development Methodologies
- 3A4. Control Identification and Design

B. Information Systems Implementation

- 3B1. Testing Methodologies
- 3B2. Configuration and Release Management
- 3B3. System Migration, Infrastructure Deployment, and Data Conversion
- 3B4. Post-Implementation Review

Content Area 4: Information Systems Operations and Business Resilience

A. Information Systems Operations

- 4A1. Common Technology Components
- 4A2. IT Asset Management
- 4A3. Job Scheduling and Production Process Automation
- 4A4. System Interfaces
- 4A5. End-User Computing
- 4A6. Data Governance
- 4A7. Systems Performance Management
- 4A8. Problem and Incident Management
- 4A9. Change, Configuration, Release, and Patch Management
- 4A10. IT Service Level Management
- 4A11. Database Management

B. Business Resilience

- 4B1. Business Impact Analysis (BIA)
- 4B2. System Resiliency
- 4B3. Data Backup, Storage, and Restoration
- 4B4. Business Continuity Plan (BCP)
- 4B5. Disaster Recovery Plans (DRP)

Trust in, and value from, information systems

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 5: Protection of Information Assets	
A.	**Information Asset Security and Control**
5A1.	Information Asset Security Frameworks, Standards, and Guidelines
5A2.	Privacy Principles
5A3.	Physical Access and Environmental Controls
5A4.	Identity and Access Management
5A5.	Network and End-Point Security
5A6.	Data Classification
5A7.	Data Encryption and Encryption-Related Techniques
5A8.	Public Key Infrastructure (PKI)
5A9.	Web-Based Communication Technologies
5A10.	Virtualized Environments
5A11.	Mobile, Wireless, and Internet-of-Things (IoT) Devices
B.	**Security Event Management**
5B1.	Security Awareness Training and Programs
5B2.	Information System Attack Methods and Techniques
5B3.	Security Testing Tools and Techniques
5B4.	Security Monitoring Tools and Techniques
5B5.	Incident Response Management
5B6.	Evidence Collection and Forensics

Supporting Tasks

1. Plan audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy.
3. Communicate audit progress, findings, results, and recommendations to stakeholders.
4. Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
5. Evaluate the IT strategy for alignment with the organization’s strategies and objectives.
6. Evaluate the effectiveness of IT governance structure and IT organizational structure.
7. Evaluate the organization’s management of IT policies and practices.
8. Evaluate the organization’s IT policies and practices for compliance with regulatory and legal requirements.
9. Evaluate IT resource and portfolio management for alignment with the organization’s strategies and objectives.
10. Evaluate the organization's risk management policies and practices.
11. Evaluate IT management and monitoring of controls.
12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
13. Evaluate the organization’s ability to continue business operations.
14. Evaluate whether the business case for proposed changes to information systems meet business objectives.
15. Evaluate whether IT supplier selection and contract management processes align with business requirements.
16. Evaluate the organization's project management policies and practices.
17. Evaluate controls at all stages of the information systems development lifecycle.
18. Evaluate the readiness of information systems for implementation and migration into production.
19. Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met.
20. Evaluate whether IT service management practices align with business requirements.
21. Conduct periodic review of information systems and enterprise architecture.
22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization’s objectives.
23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization’s objectives.
24. Evaluate database management practices.
25. Evaluate data governance policies and practices.
26. Evaluate problem and incident management policies and practices.

27. Evaluate change, configuration, release, and patch management policies and practices.

28. Evaluate end-user computing to determine whether the processes are effectively controlled.

29. Evaluate the organization's information security and privacy policies and practices.

30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.

31. Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.

32. Evaluate data classification practices for alignment with the organization’s policies and applicable external requirements.

33. Evaluate policies and practices related to asset lifecycle management.

34. Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.

35. Perform technical security testing to identify potential threats and vulnerabilities.

36. Utilize data analytics tools to streamline audit processes.

37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.

38. Identify opportunities for process improvement in the organization's IT policies and practices.

39. Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.