



CERTIFIED INFORMATION SYSTEMS AUDITOR[®]

2012 Candidate's Guide to the
CISA[®] Exam and Certification

Candidate's Guide to the CISA® Exam and Certification

CISA Exams 2012— Important Date Information

Exam Date—9 June 2012

| | |
|------------------------------|--|
| Early registration deadline: | 8 February 2012 |
| Final registration deadline: | 4 April 2012 |
| Exam registration changes: | Between 14 April and 20 April, charged a US \$50 fee, with no changes accepted after 20 April 2012 |
| Refunds: | By 13 April 2012, charged a US \$100 processing fee, with no refunds after that date |
| Deferrals: | Requests received on or before 20 April 2012, charged a US \$50 processing fee. Requests received from 21 April through 24 May 2012, charged a US \$100 processing fee. After 24 May 2012, no deferrals will be permitted. |

Exam Date—8 December 2012

| | |
|------------------------------|---|
| Early registration deadline: | 15 August 2012 |
| Final registration deadline: | 3 October 2012 |
| Exam registration changes: | Between 6 October and 12 October, charged a US \$50 fee, with no changes accepted after 12 October 2012 |
| Refunds: | By 5 October 2012, charged a US \$100 processing fee, with no refunds after that date |
| Deferrals: | Requests received on or before 12 October 2012, charged a US \$50 processing fee. Requests received from 13 October through 21 November 2012, charged a US \$100 processing fee. After 21 November 2012 no deferrals will be permitted. |

All deadlines are based upon Chicago, Illinois, USA 5 p.m. CT (central time)

ISBN 978-1-60402-229-8
2012 Candidate's Guide to the CISA® Exam and Certification
Printed in the United States of America

Table of Contents

| | |
|---|---|
| Overview | 3 |
| CISA Program Accreditation Renewed Under ISO/IEC 17024:2003 | 3 |
| The CISA Exam..... | 3 |
| Preparing for the CISA Exam | 3 |
| Administration of the CISA Exam | 4 |
| Scoring the CISA Exam..... | 6 |
| Types of Questions on the CISA Exam | 6 |
| Application for CISA Certification | 6 |
| Requirements for Initial CISA Certification | 6 |
| Requirements for Maintaining CISA Certification | 7 |
| ISACA Code of Professional Ethics | 7 |
| Revocation of CISA Certification..... | 7 |
| CISA Task and Knowledge Statements..... | 8 |

ISACA®

With 95,000 constituents in 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA and the CISA Certification Committee have designed the *2012 Candidate's Guide to the CISA® Exam and Certification* as a guide to those pursuing the CISA certification. No representations or warranties are made by ISACA that use of this guide or any other association publication will assure candidates of passing the CISA exam.

Reservation of Rights

Copyright © 2011 ISACA. Reproduction or storage in any form for any purpose is not permitted without ISACA's prior written permission. No other right or permission is granted with respect to this work. All rights reserved.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: exam@isaca.org
Web site: www.isaca.org

Candidate's Guide to the CISA® Exam and Certification

Overview

The mark of excellence for a professional certification program is the value and recognition it bestows on the individual who achieves it. Since 1978, the Certified Information Systems Auditor (CISA) program, sponsored by ISACA, has been the globally accepted standard of achievement among information systems (IS) audit, control and security professionals.

The technical skills and practices that CISA promotes and evaluates are the building blocks of success in the field. Possessing the CISA designation demonstrates proficiency and is the basis for measurement in the profession. With a growing demand for professionals possessing IS audit, control and security skills, CISA has become a preferred certification program by individuals and organizations around the world. CISA certification signifies commitment to serving an organization and the chosen profession with distinction.

CISA Program Accreditation Renewed Under ISO/IEC 17024:2003

The American National Standards Institute (ANSI) has accredited the CISA certification under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers.

ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements. ANSI describes ISO/IEC 17024 as “expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety and protecting consumers.”



ANSI's accreditation:

- Promotes the unique qualifications and expertise that ISACA certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process. With this accreditation, ISACA anticipates that significant opportunities for CISAs will continue to present themselves around the world.

The CISA Exam

Development/Description of the CISA Exam

The CISA Certification Committee oversees the development of the exam and ensures the currency of its content. Questions for the CISA exam are developed through a comprehensive process designed to enhance the ultimate quality of the exam. The process includes a Test Enhancement Subcommittee (TES) that works with item writers to develop and review questions before they are submitted to the CISA Certification Committee for review.

A job practice serves as the basis for the exam and the experience requirements to earn the CISA certification. This job practice is periodically updated and consists of five content areas (domains). The domains and the accompanying tasks and knowledge statements were the result of extensive research and feedback from subject matter experts around the world.

The tasks and knowledge statements depict the tasks performed by CISAs and the knowledge required to perform these tasks. Exam candidates will be tested based on their practical knowledge associated with performing these tasks.

The current job practice analysis contains the following domains and percentages:

- **The Process of Auditing Information Systems (14%)**
- **Governance and Management of IT (14%)**
- **Information Systems Acquisition, Development and Implementation (19%)**
- **Information Systems Operations, Maintenance and Support (23%)**
- **Protection of Information Assets (30%)**

Note: The percentages listed with the domains indicate the emphasis or percentage of questions that will appear on the exam from each domain. For a description of each domain's task and knowledge statements, please refer to pages 8-11.

The exam consists of 200 multiple-choice questions and is administered biannually in June and December during a four-hour session. Candidates may choose to take the exam in one of several languages. For a current list of languages, please visit www.isaca.org/cisaterminology.

Preparing for the CISA Exam

Passing the CISA exam can be achieved through an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates. See www.isaca.org/cisaguide to view the ISACA study aids that can help you prepare for the exam. Order early as delivery time can be from one to four weeks depending on geographic location and customs clearance practices. For current shipping information see www.isaca.org/shipping.

Candidate's Guide to the CISA® Exam and Certification



ISACA also offers a CISA® Online Review Course. The course includes interactive exercises, case studies, review tools and practice questions. Visit www.isaca.org/elearning for more information as well as a course preview.

A comprehensive list of references recommended for study can be found in the *CISA Review Manual 2012*.

A list of acronyms that candidates should be familiar with and an additional list of acronyms that candidates may wish to view can be found at www.isaca.org/cisaguide.

To assist candidates with technical terminology, a list of the most frequently used technical terms in English mapped with their translation to other languages offered is available on ISACA's web site at www.isaca.org/cisaguide.

ISACA maintains a glossary of terms as well as glossaries specific to each certification. These glossaries are available at www.isaca.org/glossary.

No representation or warranties assuring candidates' passage of the exam are made by ISACA or the CISA Certification Committee in regard to these or other association publications or courses.

Administration of the CISA Exam

ISACA utilizes an internationally recognized professional testing agency to assist the construction, administration and scoring of the CISA exam.

Candidates wishing to comment on the test administration conditions may do so at the conclusion of the testing session by completing the "Test Administration Questionnaire." The Test Administration Questionnaire is presented at the back of the examination booklet and your questionnaire answers should be entered in boxes P through S of the Special Codes section (Grid No. 4) on the front of your Answer Sheet.

Candidates who wish to address any additional comments or concerns about the examination administration, including site conditions or the content of the exam, should contact ISACA international headquarters by letter or by e-mail (exam@isaca.org). These comments or concerns are to be received by ISACA within 2 weeks after the examination date. Please include the following information in your comments: exam ID number, testing site, date tested and any relevant details on the specific issue. Only those comments received by ISACA during the first 2 weeks after the exam administration will be considered in the final scoring process of the exam.

Admission Ticket

Approximately two to three weeks prior to the CISA exam date, candidates will be sent a physical admission ticket and an e-ticket from ISACA. Exam candidates can also download a copy of the admission ticket at www.isaca.org > MyISACA page of the web site. Tickets will indicate the date, registration time and location of the exam, as well as a schedule of events for that day and a list of materials that candidates must bring with them to take the CISA exam. With the exception of contact information changes, candidates are not to write on the admission ticket.

Please Note: In order to receive an admission ticket, all fees must be paid. Admission tickets are sent via hard copy and e-mail to the current postal mailing and e-mail address on file. Only candidates with an admission ticket and an acceptable government-issued ID will be admitted to take the exam, and the name on the admission ticket must match the name on the government-issued ID. The hard copy admission ticket or print out of the e-ticket is valid for admission into the exam. If candidates' mailing and/or e-mail addresses change, they should update their profile on the ISACA web site (www.isaca.org) or contact exam@isaca.org.

It is imperative that candidates note the specific registration and exam times on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.

Any candidate who arrives after the oral instructions have begun will not be allowed to sit for the exam and will forfeit his/her registration fee. An admission ticket can only be used at the designated test center specified on the admission ticket. IDs will be checked during the exam administration.

Special Arrangements

Upon request, ISACA will make reasonable accommodations in its exam procedures for candidates with documented disabilities or religious requirements. These candidates may request consideration for reasonable alterations in exam format, presentations, food or drink at the exam site, or scheduling. Requests for food or drink at the exam site must be accompanied by a doctor's note; otherwise, **no food or drinks are allowed at any exam site**. Requests for consideration must be submitted to ISACA International Headquarters in writing, accompanied by appropriate documentation, no later than 4 April 2012 for the June 2012 exam and 3 October 2012 for the December 2012 exam.

Be Prompt

Registration will begin at the time indicated on the admission ticket at each center. All candidates must be registered and in the test center room when the chief examiner begins reading the oral instructions. **NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.**

Candidate's Guide to the CISA® Exam and Certification

Remember to Bring the Admission Ticket

Candidates can use their admission ticket (either their e-ticket or physical admission ticket) only at the designated test center. Candidates will be admitted to the test center only if they have a valid admission ticket and an acceptable form of identification (ID). An acceptable form of ID must be a current and original government-issued ID that contains the candidate's name, as it appears on the admission ticket, and the candidate's photograph. The information on the ID cannot be handwritten. All of these characteristics must be demonstrated by the single piece of ID provided. Examples include, but are not limited to, a passport, driver's license, military ID, state ID, green card and national ID. Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit his/her registration fee.

Observe the Test Center's Rules

- Candidates will not be admitted to a test center after the oral instructions have begun.
- Candidates should bring several sharpened No. 2 or HB (soft lead) pencils and a good eraser. Pencils and erasers will not be available at the test center. As exam venues vary, every attempt will be made to make the climate control comfortable at each exam venue. Candidates may want to dress to their own comfort level.
- Candidates are not allowed to bring reference materials, blank paper, note pads or language dictionaries into the test center.
- Candidates are not allowed to bring or use a calculator in the test center.
- Candidates are not allowed to bring any type of communication devices (i.e., cell phones, PDAs, Blackberries) into the test center. **If exam candidates are viewed with any such device during the exam administration, their exams will be voided and they will be asked to immediately leave the exam site.**
- Visitors are not permitted in the test center.
- No food or beverages are allowed in the test center (without advanced authorization from ISACA).

Misconduct

Candidates who are discovered engaging in any kind of misconduct—such as giving or receiving help; using notes, papers or other aids; attempting to take the exam for someone else; using any type of communication device, including cell phones, during the exam administration; or removing the exam booklet, answer sheet or notes from the testing room—will be disqualified and may face legal action. Candidates who leave the testing area without authorization or accompaniment by a test proctor will not be allowed to return to the testing room and will be subject to disqualification. The testing agency will report such irregularities to ISACA's CISA Certification Committee.

The complete Personal Belongings Policy is available at www.isaca.org/cisabelongings. Neither ISACA nor its testing vendor takes responsibility for the personal belongings of candidates.

Be Careful in Completing the Answer Sheet

- Before a candidate begins the exam, the test center chief examiner will read aloud the instructions for entering identification information on the answer sheet. A candidate's identification number as it appears on the admission ticket and all other requested information must be correctly entered or scores may be delayed or incorrectly reported.
- A proctor speaking the primary language used at each test center is available. If a candidate desires to take the exam in a language other than the primary language of the test center, the proctor may not be conversant in the language chosen. However, written instructions will be available in the language of the exam.
- A candidate is instructed to read all instructions carefully and understand them before attempting to answer the questions. Candidates who skip over the directions or read them too quickly could miss important information and possibly lose credit.
- All answers are to be marked in the appropriate circle on the answer sheet. Candidates must be careful not to mark more than one answer per question and to be sure to answer a question in the appropriate row of answers. If an answer needs to be changed, a candidate is urged to erase the wrong answer fully before marking in the new one.
- All questions should be answered. **There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly, so do not leave any questions blank.**
- After completion, candidates are required to hand in their answer sheet and test booklet.

Budget One's Time

- The exam, which is four hours in length, allows for a little over one minute per question. Candidates are advised to pace themselves to complete the entire exam. Candidates must complete an average of 50 questions per hour.
- Candidates are urged to immediately record their answers on the answer sheet. **No additional time will be allowed after the exam time has elapsed to transfer or record answers should a candidate mark answers in the test booklet.**

Conduct Oneself Properly

- To protect the security of the exam and maintain the validity of the scores, candidates are asked to sign the answer sheet.
- The CISA Certification Committee reserves the right to disqualify any candidate who is discovered engaging in any kind of misconduct or violation of exam rules, such as giving or receiving help; using notes, papers or other aids; attempting to take the exam for someone else; or removing test materials or notes from the test center. The testing agency will provide the CISA Certification Committee with records regarding such irregularities for their review and to render a decision.

Candidate's Guide to the CISA® Exam and Certification

Reasons for Dismissal or Disqualification

- Unauthorized admission to the test center.
- Candidate creates a disturbance or gives or receives help.
- Candidate attempts to remove test materials or notes from the test center.
- Candidate impersonates another candidate.
- Candidate brings items into the test center that are not permitted.
- Candidate possession of any communication device (i.e., cell phone, PDA, BlackBerry®) during the exam administration
- Candidate unauthorized leave of the test area

If candidates are observed with any communication device (i.e., cell phone, PDA, BlackBerry) during the exam administration, their exams will be voided and they will be asked to immediately leave the test site.

Scoring the CISA Exam

The CISA exam consists of 200 multiple-choice items. Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. ISACA uses and reports scores on a common scale from 200 to 800. For example, the scaled score of 800 represents a perfect score with all questions answered correctly; a scaled score of 200 is the lowest score possible and signifies that only a small number of questions were answered correctly. A candidate must receive a score of 450 or higher to pass the exam. A score of 450 represents a minimum consistent standard of knowledge as established by the CISA Certification Committee. A candidate receiving a passing score may then apply for certification if all other requirements are met.

The CISA exam contains some questions which are included for research and analysis purposes only. These questions are not separately identified and not used to calculate your final score.

Approximately eight weeks after the test date, the official exam results will be mailed to candidates. Additionally, with the candidate's consent during the registration process, an e-mail message containing the candidate's pass/fail status and score will be sent to the candidate. This e-mail notification will only be sent to the address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax. To prevent e-mail notification from being sent to spam folders, candidates should add *exam@isaca.org* to their address book, whitelist or safe-senders list.

Candidates will receive a score report containing a subscore for each domain area. Successful candidates will receive, along with a score report, details on how to apply for CISA certification.

The subscores can be useful in identifying those areas in which the unsuccessful candidate may need further study before retaking the exam. Unsuccessful candidates should note that the total scaled score cannot be determined by calculating either a simple or weighted average of the subscores.

Candidates receiving a failing score on the exam may request a hand score of their answer sheets. This procedure ensures that no stray marks, multiple responses or other conditions interfered with computer scoring. Candidates should understand, however, that all scores are subjected to several quality control checks before they are reported; therefore, rescores most likely will not result in a score change. Requests for hand scoring must be made in writing to the certification department within 90 days following the release of the exam results. Requests for a hand score after the deadline date will not be processed. All requests must include a candidate's name, exam identification number and mailing address. A fee of US \$75 must accompany each request.

Types of Questions on the CISA Exam

CISA exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. All questions are designed with one best answer.

Every CISA question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. The candidate is cautioned to read each question carefully. A CISA exam question may require the candidate to choose the appropriate answer based on a qualifier, such as **MOST** likely or **BEST**. In every case, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Representations of CISA exam questions are available at www.isaca.org/cisaassessment.

Application for CISA Certification

Passing the exam does not mean a candidate is a CISA. Once a candidate passes the CISA exam, he/she has five years from the date of the exam to apply for certification. Successful candidates must complete the application for certification and have their work experience verified using the appropriate forms included in the application. **Candidates are not certified, and cannot use the CISA designation, until the completed application is received and approved.** Please note that decisions on applications are not final as there is an appeal process for certification application denials. Inquiries regarding denials of certification can be sent to certification@isaca.org. Once certified, the new CISA will receive a certificate and CISA certification pin. At the time of application, individuals must also acknowledge that ISACA reserves the right, but is not obligated, to publish or otherwise disclose their CISA status. A processing fee of US \$50 must accompany your CISA Application for Certification.

Candidate's Guide to the CISA® Exam and Certification

Requirements for Initial CISA Certification

Certification is granted initially to individuals who have completed the CISA exam successfully and meet the following work experience requirements.

A minimum of five years of professional IS audit, control, assurance or security work experience is required for certification. Substitutions and waivers of such experience may be obtained as follows:

- A maximum of one year of information systems OR one year of non-IS auditing experience can be substituted for one year of experience.
- Sixty to 120 completed university semester credit hours (the equivalent of a two-year or four-year degree), not limited by the 10-year preceding restriction, can be substituted for one or two years, respectively, of experience. Even if multiple degrees have been earned, a maximum of two years can be claimed.
- A bachelor's or master's degree from a university that enforces the ISACA-sponsored Model Curriculum can be substituted for one year of experience. To view a list of these schools, please visit www.isaca.org/modeluniversities. This option cannot be used if three years of experience substitution and educational waiver have already been claimed.
- A master's degree in information security or information technology from an accredited university can be substituted for one year of experience.

Exception: Two years as a full-time university instructor in a related field (e.g., computer science, accounting, information systems auditing) can be substituted for every one year of experience.

Experience must have been gained within the 10-year period preceding the date of the application for CISA certification or within five years from the date of initially passing the exam. If a complete application for CISA certification is not submitted within five years from the passing date of the exam, retaking and passing the exam is required.

It is important to note that many individuals choose to take the CISA exam prior to meeting the experience requirements. This practice is acceptable and encouraged, although the CISA designation will not be awarded until all requirements are met.

Requirements for Maintaining CISA Certification

CISAs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 CPE hours, and attain and report a minimum of 120 CPE hours for a three-year reporting period. For more details visit the CISA CPE policy at www.isaca.org/cisacpepolicy.
- Submit annual CPE maintenance fees in full to ISACA International Headquarters.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with the ISACA Code of Professional Ethics.

Failure to comply with these general requirements will result in the revocation of an individual's CISA designation. All certificates are owned by ISACA. If an individual is approved for certification and subsequently revoked, the individual must destroy the certificate.

ISACA Code of Professional Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders. Failure to comply with this Code of Professional Ethics can result in an investigation into a member's and/or certification holder's conduct and, ultimately, in disciplinary measures. The ISACA Code of Professional Ethics can be viewed online at www.isaca.org/ethics.

Revocation of CISA Certification

The CISA Certification Committee may, at its discretion after due and thorough consideration, revoke an individual's CISA certification for any of the following reasons:

- Failing to comply with the CISA CPE policy
- Violating any provision of the ISACA Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CISA exam or the certification process

Candidate's Guide to the CISA® Exam and Certification

Description of CISA Job Practice Areas CISA Task and Knowledge Statements

| CONTENT AREA (Domain) | |
|--|--|
| Domain 1: The Process of Auditing Information Systems —Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems. | |
| Domain 1: Task Statements | |
| T1.1 | Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included. |
| T1.2 | Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization. |
| T1.3 | Conduct audits in accordance with IT audit standards to achieve planned audit objectives. |
| T1.4 | Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary. |
| T1.5 | Conduct follow-ups or prepare status reports to ensure that appropriate actions have been taken by management in a timely manner. |
| Domain 1: Knowledge Statements | |
| KS1.1 | Knowledge of ISACA IT Audit and Assurance Standards, Guidelines, and Tools and Techniques; Code of Professional Ethics, and other applicable standards |
| KS1.2 | Knowledge of risk assessment concepts, tools and techniques in an audit context |
| KS1.3 | Knowledge of control objectives and controls related to information systems |
| KS1.4 | Knowledge of audit planning and audit project management techniques, including follow-up |
| KS1.5 | Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT |
| KS1.6 | Knowledge of applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits |
| KS1.7 | Knowledge of evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis) used to gather, protect and preserve audit evidence |
| KS1.8 | Knowledge of different sampling methodologies |
| KS1.9 | Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure) |
| KS1.10 | Knowledge of audit quality assurance systems and frameworks |
| Domain 2: Governance and Management of IT —Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy. | |
| Domain 2: Task Statements | |
| T2.1 | Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives. |
| T2.2 | Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives. |
| T2.3 | Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives. |
| T2.4 | Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements. |
| T2.5 | Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner. |
| T2.6 | Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures. |
| T2.7 | Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives. |
| T2.8 | Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives. |
| T2.9 | Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed. |
| T2.10 | Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance. |
| T2.11 | Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption. |

Candidate's Guide to the CISA® Exam and Certification

| CONTENT AREA (Domain) | |
|--|---|
| Domain 2: Knowledge Statements | |
| KS2.1 | Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines, and practices |
| KS2.2 | Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each |
| KS2.3 | Knowledge of organizational structure, roles and responsibilities related to IT |
| KS2.4 | Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures |
| KS2.5 | Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions |
| KS2.6 | Knowledge of relevant laws, regulations and industry standards affecting the organization |
| KS2.7 | Knowledge of quality management systems |
| KS2.8 | Knowledge of the use of maturity models |
| KS2.9 | Knowledge of process optimization techniques |
| KS2.10 | Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management) |
| KS2.11 | Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third-party outsourcing relationships |
| KS2.12 | Knowledge of enterprise risk management |
| KS2.13 | Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPIs]) |
| KS2.14 | Knowledge of IT human resources (personnel) management practices used to invoke the business continuity plan |
| KS2.15 | Knowledge of business impact analysis (BIA) related to business continuity planning (BCP) |
| KS2.16 | Knowledge of the standards and procedures for the development and maintenance of the business continuity plan (BCP) and testing methods |
| Domain 3: Information Systems Acquisition, Development and Implementation —Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives. | |
| Domain 3: Task Statements | |
| T3.1 | Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives. |
| T3.2 | Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization. |
| T3.3 | Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate. |
| T3.4 | Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements. |
| T3.5 | Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met. |
| T3.6 | Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met. |
| Domain 3: Knowledge Statements | |
| KS3.1 | Knowledge of benefits realization practices (e.g., feasibility studies, business cases, total cost of ownership [TCO], ROI) |
| KS3.2 | Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office) |
| KS3.3 | Knowledge of project management control frameworks, practices and tools |
| KS3.4 | Knowledge of risk management practices applied to projects |
| KS3.5 | Knowledge of IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, <i>n</i> -tier applications) |
| KS3.6 | Knowledge of acquisition practices (e.g., evaluation of vendors, vendor management, escrow) |
| KS3.7 | Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements) |
| KS3.8 | Knowledge of project success criteria and risks |
| KS3.9 | Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data |

Candidate's Guide to the CISA® Exam and Certification

| CONTENT AREA (Domain) |
|---|
| Domain 3: Knowledge Statements (cont.) |
| KS3.10 Knowledge of system development methodologies and tools, including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques) |
| KS3.11 Knowledge of testing methodologies and practices related to information systems development |
| KS3.12 Knowledge of configuration and release management relating to the development of information systems |
| KS3.13 Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures |
| KS3.14 Knowledge of postimplementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement) |
| Domain 4: Information Systems Operations, Maintenance and Support —Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives. |
| Domain 4: Task Statements |
| T4.1 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives. |
| T4.2 Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed. |
| T4.3 Evaluate third-party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider. |
| T4.4 Evaluate operations and end-user procedures to determine whether scheduled and nonscheduled processes are managed to completion. |
| T4.5 Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives. |
| T4.6 Evaluate data administration practices to determine the integrity and optimization of databases. |
| T4.7 Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives. |
| T4.8 Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner. |
| T4.9 Evaluate change, configuration and release management practices to determine whether scheduled and nonscheduled changes made to the organization's production environment are adequately controlled and documented. |
| T4.10 Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing. |
| T4.11 Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster. |
| Domain 4: Knowledge Statements |
| KS4.1 Knowledge of service level management practices and the components within a service level agreement |
| KS4.2 Knowledge of techniques for monitoring third-party compliance with the organization's internal controls |
| KS4.3 Knowledge of operations and end-user procedures for managing scheduled and nonscheduled processes |
| KS4.4 Knowledge of the technology concepts related to hardware and network components, system software, and database management systems |
| KS4.5 Knowledge of control techniques that ensure the integrity of system interfaces |
| KS4.6 Knowledge of software licensing and inventory practices |
| KS4.7 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering) |
| KS4.8 Knowledge of database administration practices |
| KS4.9 Knowledge of capacity planning and related monitoring tools and techniques |
| KS4.10 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing) |
| KS4.11 Knowledge of problem and incident management practices (e.g., help desk, escalation procedures, tracking) |
| KS4.12 Knowledge of processes for managing scheduled and nonscheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices |
| KS4.13 Knowledge of data backup, storage, maintenance, retention and restoration practices |
| KS4.14 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery |

Candidate's Guide to the CISA® Exam and Certification

| CONTENT AREA (Domain) |
|--|
| Domain 4: Knowledge Statements (cont.) |
| KS4.15 Knowledge of business impact analysis (BIA) related to disaster recovery planning |
| KS4.16 Knowledge of the development and maintenance of disaster recovery plans |
| KS4.17 Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites) |
| KS4.18 Knowledge of processes used to invoke the disaster recovery plans |
| KS4.19 Knowledge of disaster recovery testing methods |
| Domain 5: Protection of Information Assets —Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets. |
| Domain 5: Task Statements |
| T5.1 Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices. |
| T5.2 Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information. |
| T5.3 Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements. |
| T5.4 Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded. |
| T5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data and softcopy media) to determine whether information assets are adequately safeguarded. |
| Domain 5: Knowledge Statements |
| KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security controls, including security awareness programs |
| KS5.2 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team) |
| KS5.3 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data |
| KS5.4 Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems), and database management systems |
| KS5.5 Knowledge of risks and controls associated with virtualization of systems |
| KS5.6 Knowledge of the configuration, implementation, operation and maintenance of network security controls |
| KS5.7 Knowledge of network and Internet security devices, protocols and techniques |
| KS5.8 Knowledge of information system attack methods and techniques |
| KS5.9 Knowledge of detection tools and control techniques (e.g., malware, virus detection, spyware) |
| KS5.10 Knowledge of security testing techniques (e.g., intrusion testing, vulnerability scanning) |
| KS5.11 Knowledge of risks and controls associated with data leakage |
| KS5.12 Knowledge of encryption-related techniques |
| KS5.13 Knowledge of public key infrastructure (PKI) components and digital signature techniques |
| KS5.14 Knowledge of risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs) |
| KS5.15 Knowledge of controls and risks associated with the use of mobile and wireless devices |
| KS5.16 Knowledge of voice communications security (e.g., PBX, VoIP) |
| KS5.17 Knowledge of the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody) |
| KS5.18 Knowledge of data classification standards and supporting procedures |
| KS5.19 Knowledge of physical access controls for the identification, authentication and restriction of users to authorized facilities |
| KS5.20 Knowledge of environmental protection devices and supporting practices |
| KS5.21 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets |



Prepare for the 2012 CISA Exams

2012 CISA Review Resources for Exam Preparation and Professional Development

Successful Certified Information Systems Auditor® (CISA®) exam candidates have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates. These include:

Study Aids

- *CISA® Review Manual 2012*
- *CISA® Review Questions, Answers & Explanations Manual 2011*
- *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement*
- *CISA® Review Questions, Answers & Explanations Manual 2012 Supplement*
- CISA® Practice Question Database v12

To order, visit www.isaca.org/cisabooks.

Review Courses

- Chapter-sponsored review courses (www.isaca.org/cisareview)
- CISA® Online Review Course (www.isaca.org/elearning)

