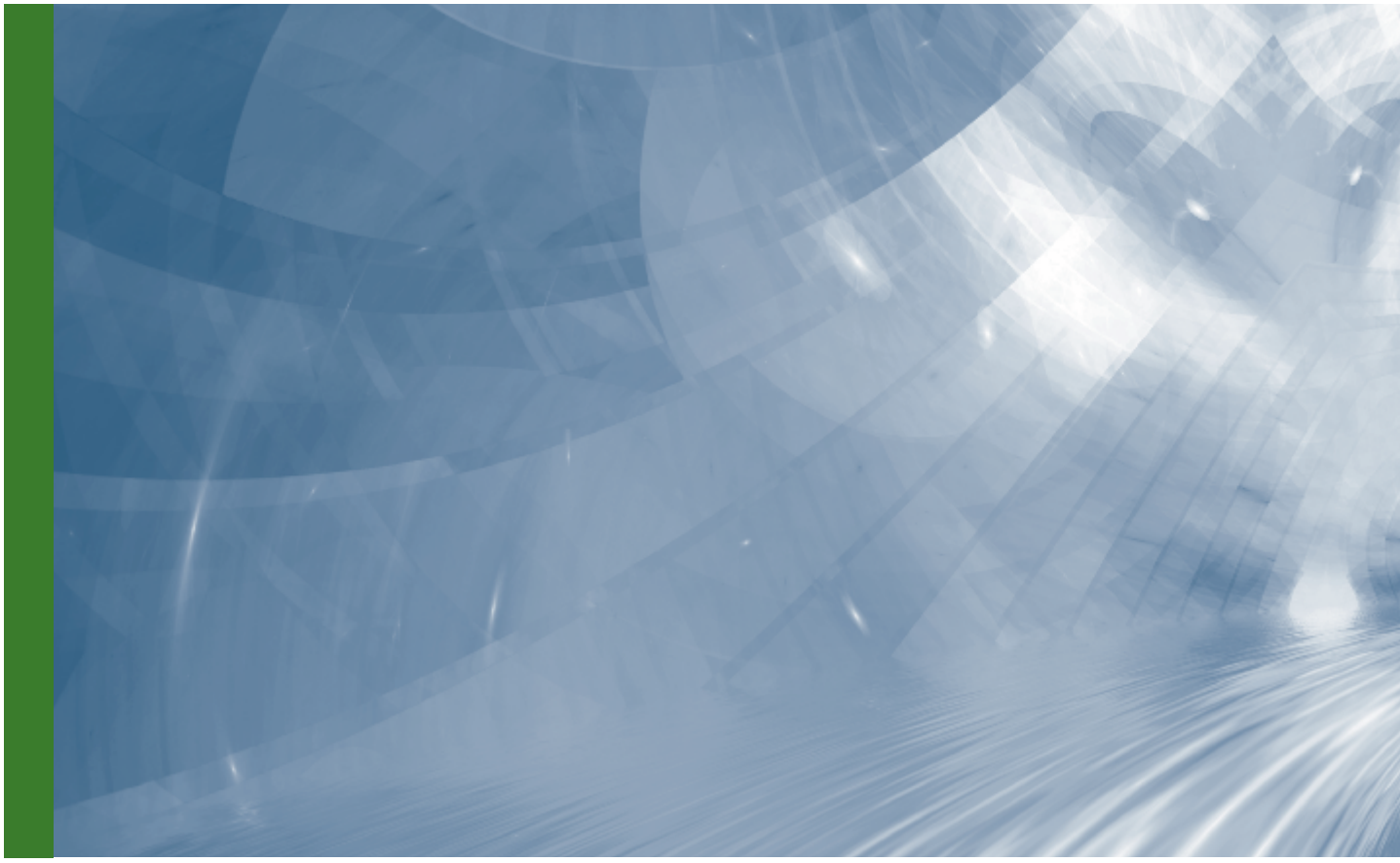
ISACA®

Certified Information Systems Auditor™

An ISACA Certification



Candidate's Guide to the CISA® Exam and Certification

CISA®
Certified Information Systems Auditor

CISA Exams 2010—Important Date Information

Exam Date—12 June 2010

Early registration deadline:	10 February 2010
Final registration deadline:	7 April 2010
Exam registration changes:	Between 17 April and 23 April, charged a US $50 fee, with no changes accepted after 23 April 2010
Refunds:	By 16 April 2010, charged a US $100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 23 April 2010, charged a US $50 processing fee. Requests received from 24 April through 27 May 2010, charged a US $100 processing fee. After 27 May 2010, no deferrals will be permitted.

Exam Date—11 December 2010

Early registration deadline:	18 August 2010
Final registration deadline:	6 October 2010
Exam registration changes:	Between 9 October and 15 October, charged a US $50 fee, with no changes accepted after 15 October 2010
Refunds:	By 8 October 2010, charged a US $100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 15 October 2010, charged a US $50 processing fee. Requests received from 16 October through 24 November 2010, charged a US $100 processing fee. After 24 November 2010, no deferrals will be permitted.

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

Table of Contents

Overview 3
CISA Program Accreditation Renewed Under ISO/IEC 17024:2003 3
The CISA Exam 3
Preparing for the CISA Exam 4
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 Knowledgement Statements 8

ISACA®
With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA Journal*®, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 10,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT® (CGEIT®) designation.

Disclaimer
ISACA and the CISA Certification Board have designed the *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.

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*

ISBN 978-1-60420-120-8
Candidate's Guide to the CISA Exam and Certification
Printed in the United States of America..

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 Accredited Program
PERSONNEL CERTIFICATION
#0694
ISO/IEC 17024

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 six 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 IS Audit Process (10%)**
- **IT Governance (15%)**
- **Systems and Infrastructure Life Cycle Management (16%)**
- **IT Service Delivery and Support (14%)**
- **Protection of Information Assets (31%)**
- **Business Continuity and Disaster Recovery (14%)**

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.*

Although knowledge of *Control Objectives for Information and related Technology* (CobiT®) is not specifically tested on the CISA exam, the CobiT control objectives or processes are reflected in the CISA job practice task statements. As such, a thorough review of CobiT is recommended for candidate preparation for the CISA exam. To focus a candidate's attention on the specific CobiT processes that relate to CISA practice analysis tasks, go to *www.isaca.org/cisaguide.*

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*.

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 list of references recommended for further study in preparation for the exam can be found at *www.isaca.org/cisaguide*. A more comprehensive list can be found in the *CISA Review Manual 2009*.

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/examterm.*

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 should contact ISACA international head-quarters by letter or by e-mail (exam@isaca.org). These comments or concerns should be received by ISACA within 2 weeks after the examination date.

Candidates who wish to comment on the contents of the examination may do so by mailing their comments to the Professional Examination Service. However, only those comments received by The Professional Examination Service during the first 2 weeks after the exam administration will be considered in the final scoring process of the examination. You may obtain the address of the Professional Examination Service from the Proctor after you complete the examination.

Admission Ticket

Approximately two to three weeks prior to the CISA exam date, candidates will receive a physical admission ticket and an e-ticket from ISACA. 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.

Please Note: In order to receive a hard copy admission ticket, all fees must be paid. In order to receive an e-ticket, all fees must be paid and candidates must have a current e-mail address on file. Only candidates with an admission ticket will be admitted to the exam. Both the hard copy admission ticket and e-ticket are valid for the exam. If a candidate's mailing and/or e-mail address changes, he/she should update his/her 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.

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**. Request for consideration must be submitted to ISACA International Headquarters in writing, accompanied by appropriate documentation, no later than 7 April 2010 for the June 2010 exam and 6 October 2010 for the December 2010 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 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.**

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.
- Candidates are not allowed to bring reference materials, blank paper 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.
- Visitors are not permitted in the test center.
- No food or beverages are allowed in the test center.

The complete Personal Belongings Policy is available at *www.isaca.org/cisabelongings*.

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, 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.

Reasons for Dismissal
The proctor may dismiss a candidate for any of the following reasons:
- 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 brings items into the test center that are not permitted.

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 on the registration form, 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. Unsuccessful candidates will receive, along with a score report, a copy of the new CISA Bulletin of Information.

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 $65 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.** Once certified, the new CISA will receive a certificate and the CISA continuing professional education (CPE) policy requirements. 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.

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 the 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. The CISA CPE policy (*www.isaca.org/cisacpepolicy*) requires the attainment of CPE hours over an annual and three-year reporting period.
- Attain and report a minimum of 120 CPE hours for a three-year reporting period.
- 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.

ISACA Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:
1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities that they can reasonably expect to complete with professional competence
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control

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.

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

Description of CISA Job Practice Areas
CISA Task and Knowledge Statements

CONTENT AREA (Domain)
1. The IS Audit Process—Provide IS audit services in accordance with IS audit standards, guidelines and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.
Task Statements
1.1 Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.
1.2 Plan specific audits to ensure that IT and business systems are protected and controlled.
1.3 Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
1.4 Communicate emerging issues, potential risks and audit results to key stakeholders.
1.5 Advise on the implementation of risk management and control practices within the organization, while maintaining independence.
Knowledge Statements
1.1 Knowledge of ISACA IS Auditing Standards, Guidelines and Procedures and the Code of Professional Ethics
1.2 Knowledge of IS auditing practices and techniques
1.3 Knowledge of techniques to gather information and preserve evidence (e.g., observation, inquiry, interview, CAATTs and electronic media)
1.4 Knowledge of the evidence life cycle (e.g., the collection, protection, chain of custody)
1.5 Knowledge of control objectives and controls related to IS (e.g., CobiT)
1.6 Knowledge of risk assessment in an audit context
1.7 Knowledge of audit planning and management techniques
1.8 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation and conflict resolution)
1.9 Knowledge of control self-assessment (CSA)
1.10 Knowledge of continuous audit techniques
2. IT Governance—Provide assurance that the organization has the structure, policies, accountability, mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.
Task Statements
2.1 Evaluate the effectiveness of the IT governance structure to ensure adequate board control over the decisions, directions and performance of IT so that it supports the organization's strategies and objectives.
2.2 Evaluate the IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.
2.3 Evaluate the IT strategy and the process for its development, approval, implementation and maintenance to ensure that it supports the organization's strategies and objectives.
2.4 Evaluate the organization's IT policies, standards and procedures and the processes for their development, approval, implementation and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.
2.5 Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standard and procedures.
2.6 Evaluate IT resource investment, use and allocation practices to ensure alignment with the organization's strategies and objectives.
2.7 Evaluate IT contracting strategies and policies and contract management practices to ensure that they support the organization's strategies and objectives.
2.8 Evaluate risk management practices to ensure that the organization's IT-related risks are properly managed.
2.9 Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.
Knowledge Statements
2.1 Knowledge of the purpose of IT strategies, policies, standards and procedures for an organization and the essential elements of each
2.2 Knowledge of IT governance frameworks
2.3 Knowledge of the processes for the development, implementation and maintenance of IT strategies, policies, standards and procedures (e.g., protection of information assets, business continuity and disaster recovery, systems and infrastructure life cycle management, and IT service delivery and support)
2.4 Knowledge of quality management strategies and policies
2.5 Knowledge of organizational structure, roles and responsibilities related to the use and management of IT
2.6 Knowledge of generally accepted international IT standards and guidelines
2.7 Knowledge of enterprise IT architecture and its implications for setting long-term strategic goals
2.8 Knowledge of risk management methodologies and tools
2.9 Knowledge of the use of control frameworks (e.g., CobiT, COSO and ISO/IEC 17799)

CONTENT AREA (Domain)
2. IT Governance (*continued*)
2.10 Knowledge of the use of maturity and process improvement models (e.g., CMM and CobiT)
2.11 Knowledge of contracting strategies, processes and contract management practices
2.12 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards and key performance indicators)
2.13 Knowledge of relevant legislative and regulatory issues (e.g., privacy, intellectual property and corporate governance requirements)
2.14 Knowledge of IT human resources (personnel) management
2.15 Knowledge of IT resource investment and allocation practices (e.g., portfolio management return on investment)
3. Systems and Infrastructure Life Cycle Management—Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance and disposal of systems and infrastructure will meet the organization's objectives.
Task Statements
3.1 Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organization's business goals.
3.2 Evaluate the project management framework and project governance practices to ensure that business objectives are achieved in a cost-effective manner, while managing risks to the organization.
3.3 Perform reviews to ensure that a project is progressing in accordance with project plans, is adequately supported by documentation and its status reporting is accurate.
3.4 Evaluate proposed control mechanisms for systems and/or infrastructure during specification, development/acquisition and testing to ensure that they will provide safeguards and comply with the organization's policies and other requirements.
3.5 Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organization's objectives.
3.6 Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.
3.7 Perform postimplementation review of systems and/or infrastructure to ensure that they meet the organization's objectives and are subject to effective internal control.
3.8 Perform periodic reviews of systems and/or infrastructure to ensure that they continue to meet the organization's objectives and are subject to effective internal control.
3.9 Evaluate the process by which systems and/or infrastructure are maintained to ensure the continued support of the organization's objectives and that the systems and/or infrastructure are subject to effective internal control.
3.10 Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organization's policies and procedures.
Knowledge Statements
3.1 Knowledge of benefits management practice (e.g., feasibility studies and business cases)
3.2 Knowledge of project governance mechanisms (e.g., steering committee and project oversight board)
3.3 Knowledge of project management practices, tools and control frameworks
3.4 Knowledge of risk management practices applied to projects
3.5 Knowledge of project success criteria and risks
3.6 Knowledge of configuration, change and release management in relation to development and maintenance of systems and/or infrastructure
3.7 Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data within IT systems applications
3.8 Knowledge of enterprise architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services and n-tier applications)
3.9 Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability and gap analysis)
3.10 Knowledge of acquisition and contract management processes (e.g., evaluation of vendors, preparation of contracts, vendor management and escrow)
3.11 Knowledge of system development methodologies and tools and an understanding of their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development and object-oriented design techniques)
3.12 Knowledge of quality assurance methods
3.13 Knowledge of the management of testing processes (e.g., test strategies, test plans, test environments, entry and exit criteria)
3.14 Knowledge of data conversion tools, techniques and procedures
3.15 Knowledge of system and/or infrastructure disposal procedures
3.16 Knowledge of software and hardware certification and accreditation practices
3.17 Knowledge of postimplementation review objectives and methods (e.g., project closure, benefits realization and performance measurement)
3.18 Knowledge of system migration and infrastructure deployment practices

CONTENT AREA (Domain)
4. IT Service Delivery and Support—Provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.
Task Statements
4.1 Evaluate service-level management practices to ensure that the level of service from internal and external service providers is defined and managed.
4.2 Evaluate operations management to ensure that IT support functions effectively meet business needs.
4.3 Evaluate data administration practices to ensure the integrity and optimization of databases.
4.4 Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives.
4.5 Evaluate change, configuration and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented.
4.6 Evaluate problem and incident management practices to ensure that incidents, problems and errors are recorded, analyzed and resolved in a timely manner.
4.7 Evaluate the functionality of the IT infrastructure (e.g., network components, hardware and system software) to ensure that it supports the organization's objectives.
Knowledge Statements
4.1 Knowledge of service-level management practices
4.2 Knowledge of operations management best practices (e.g., workload scheduling, network services management and preventive maintenance)
4.3 Knowledge of system performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports and load balancing)
4.4 Knowledge of the functionality of hardware and network components (e.g., routers, switches, firewalls and peripherals)
4.5 Knowledge of database administration practices
4.6 Knowledge of the functionality of system software including operating systems, utilities and database management systems
4.7 Knowledge of capacity planning and monitoring techniques
4.8 Knowledge of processes for managing scheduled and emergency changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
4.9 Knowledge of incident/problem management practices (e.g., help desk, escalation procedures and tracking)
4.10 Knowledge of software licensing and inventory practices
4.11 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure and clustering)
5. Protection of Information Assets—Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.
Task Statements
5.1 Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.
5.2 Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.
5.3 Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.
5.4 Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.
5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.
Knowledge Statements
5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis and privacy impact assessment)
5.2 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus and profiles)
5.3 Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies and identity management)
5.4 Knowledge of attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service and spamming)
5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures and emergency incident response teams)
5.6 Knowledge of network and Internet security devices, protocols and techniques (e.g., SSL, SET, VPN and NAT)
5.7 Knowledge of intrusion detection systems and firewall configuration, implementation, operation and maintenance
5.8 Knowledge of encryption algorithm techniques (e.g., AESRSA)
5.9 Knowledge of public key infrastructure (PKI) components (e.g., certification authorities and registration authorities) and digital signature techniques

CONTENT AREA (Domain)
5. Protection of Information Assets (*continued*)
5.10 Knowledge of virus detection tools and control techniques
5.11 Knowledge of security testing and assessment tools (e.g., penetration testing and vulnerability scanning)
5.12 Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems and water sensors)
5.13 Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks and tokens)
5.14 Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data)
5.15 Knowledge of voice communications security (e.g., voiceover IP)
5.16 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., PDAs, USB devices and Bluetooth devices)
6. Business Continuity and Disaster Recovery—Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services, while minimizing the business impact.
Task Statements
6.1 Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing.
6.2 Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.
6.3 Evaluate the organization's business continuity plan to ensure its ability to continue essential business operations during the period of an IT disruption.
Knowledge Statements
6.1 Knowledge of data backup, storage, maintenance, retention and restoration processes and practices
6.2 Knowledge of regulatory, legal, contractual and insurance issues related to business continuity and disaster recovery
6.3 Knowledge of business impact analysis (BIA)
6.4 Knowledge of the development and maintenance of the business continuity and disaster recovery plans
6.5 Knowledge of business continuity and disaster recovery testing approaches and methods
6.6 Knowledge of human resources management practices as related to business continuity and disaster recovery (e.g., evacuation planning and response teams)
6.7 Knowledge of processes used to invoke the business continuity and disaster recovery plans
6.8 Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites and cold sites)

Prepare for the **2010** *CISA Exams*

ORDER NOW—2010 CISA® Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Systems Auditor™ (CISA) exam, candidates should 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 (*www.isaca.org/cisareview*) to exam candidates.

CISA Review Manual 2010

ISACA

The *CISA® Review Manual 2010* is a comprehensive reference guide designed to assist individuals in preparing for the CISA exam and individuals who wish to understand the roles and responsibilities of an information systems auditor. The manual has evolved over the past editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

The *CISA Review Manual 2010* features a new format. Each of the six chapters has been divided into two sections for focused study. The first section of each chapter contains the definitions and objectives for the six areas, with the corresponding tasks performed by information systems (IS) auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam.

Section One is an overview that provides:
- Definitions for the six areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in Section Two for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section Two consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam. In addition, the *CISA Review Manual 2010* includes brief chapter summaries focused on the main topics and case studies to assist candidates in understanding current practices. Also included are definitions of terms most commonly found on the exam.

This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- IS audit process
- IT governance
- Systems and infrastructure life cycle management
- IT service delivery and support
- Protection of information assets
- Business continuity and disaster recovery

CRM-10	English Edition	**CRM-10J**	Japanese Edition
CRM-10F	French Edition	**CRM-10S**	Spanish Edition
CRM-10I	Italian Edition		

CISA Review Questions, Answers & Explanations Manual 2010

ISACA

The *CISA® Review Questions, Answers & Explanations Manual 2010* consists of 800 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2008* and the *2008* and *2009 Supplements*. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISA exam question format, and/or provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISA Review Manual 2010.*

To assist candidates in maximizing study efforts, questions are presented in the following two ways:
- Sorted by job practice area
- Scrambled as a sample 200-question exam

QAE-10	English Edition	**QAE-10J**	Japanese Edition
QAE-10I	Italian Edition	**QAE-10S**	Spanish Edition

CISA Review Questions, Answers & Explanations Manual 2010 Supplement

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2010 Supplement* is recommended for use when preparing for the 2010 CISA exam. This supplement consists of 100 new sample questions, answers and explanations based on the current CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide CISA candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

QAE-10ES	English Edition	**QAE-10JS**	Japanese Edition
QAE-10FS	French Edition	**QAE-10SS**	Spanish Edition
QAE-10IS	Italian Edition		

CISA Practice Question Database v10

ISACA

The CISA® Practice Question Database v10 combines the *CISA Review Questions, Answers & Explanations Manual 2010* with the *CISA Review Questions, Answers & Explanations Manual 2010 Supplement* into one comprehensive 900-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

CDB-10	English Edition—CD-ROM
CDB-10W	English Edition—Download
CDB-10S	Spanish Edition—CD-ROM
CDB-10SW	Spanish Edition—Download

CISA Online Review Course

ISACA

A complete web-based exam review course is available at *www.isaca.org/elearning.*

To order CISA review material for the June/December 2010 exams, visit the ISACA web site at *www.isaca.org/cisabooks.*

ISBN 978-1-60420-120-8
90000
9 781604 201208