



**Candidate's Guide to the
CISA® Exam and Certification**

Candidate's Guide to the CISA Exam and Certification

ISACA®

With more than 65,000 members in more than 140 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 *Information Systems Control 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 50,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by 7,000 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* 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.

Disclosure

Copyright © 2007 Information Systems Audit and Control Association. 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: examregistrant@isaca.org
Web site: www.isaca.org

ISBN 978-1-60420-062-1

Candidate's Guide to the CISA Exam

Printed in the United States of America.

Table of Contents

Introduction	2
CISA Program Accreditation Renewed Under ISO/IEC 17024:2003	2
The CISA Exam	2
Content of the CISA Exam	3
Administration of the CISA Exam	3
Scoring the CISA Exam	5
Types of Questions on the CISA Exam	5
CISA Exam Terminology	6
Application for CISA Certification	6
Requirements for Initial CISA Certification	7
Requirements for Maintaining CISA Certification	7
Revocation of CISA Certification	7
ISACA Code of Professional Ethics	8
CISA Task and Knowledge Statements	9
The CISA Exam and COBIT	14
Suggested Resources for Further Study	15
List of Acronyms	18
Sample Admission Ticket	22
Sample Answer Sheet	23

Candidate's Guide to the CISA Exam and Certification

Introduction

The Certified Information Systems Auditor™ (CISA®) program was established in 1978 to:

- Develop and maintain a testing instrument that could be used to evaluate an individual's competency in conducting information systems audits
- Provide a mechanism for motivating information systems auditors to maintain their competencies and monitoring the success of the maintenance programs
- Aid top management in developing a sound information systems audit function by providing criteria for personnel selection and development

The CISA program is designed to assess and certify individuals in the IS audit, control or security profession who demonstrate exceptional skill, judgment and proficiency in IS audit, control and security practices.

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

The detailed job content areas, developed by an experienced and representative panel of CISAs, serve as a syllabus for the CISA exam. Although the tasks and knowledge statements are intended to be reasonably comprehensive, candidates are encouraged to investigate additional tasks not specifically listed but appropriate. In the review of these statements, candidates should use discretion as to the depth of coverage and the amount of time to dedicate to any given area.

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

Candidate's Guide to the CISA Exam and Certification

Content of the CISA Exam

The content of the exam is continuously modified to reflect changes in technology and practices. Every five years or sooner, a thorough job practice analysis is conducted to determine the tasks and knowledge required of individuals aspiring to become CISAs. The most recent job practice analysis, completed in 2004, resulted in the following content areas 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 practice areas indicate the emphasis or percent of questions that will appear on the exam from each area.

Each practice area's definition, tasks and knowledge statements are included in the table on page 9.

Study Aids for the CISA Exam

ISACA offers CISA candidates many study aid options including a review manual and sample review questions, answers and explanations. See www.isaca.org/cisaguide to view the ISACA study aids that can help you with your preparation of a successful study plan. Order early as delivery time can be from one to four weeks depending on geographic location and custom clearance practices. For current shipping information see www.isaca.org/shipping.

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

Administration of the CISA Exam

ISACA has contracted with an internationally recognized professional testing agency. This not-for-profit corporation engages in the development and administration of credentialing exams for certification and licensing purposes. It assists ISACA in the construction, administration and scoring of the CISA exam.

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 candidates must bring with them to take the CISA exam.

Please Note: In order to receive an e-ticket, candidates must have a current e-mail address on file. If a candidate's e-mail address changes, he/she should update his/her profile on the ISACA web site (www.isaca.org) or contact examregistrant@isaca.org.

It is imperative that candidates note the specific registration and exam time on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS 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.

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.**

Candidate's Guide to the CISA Exam and Certification

Remember to Bring the Admission Ticket

Candidates can use their admission ticket only at the designated test center. Only those candidates with a **valid admission ticket and an acceptable form of original identification** will be admitted. 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 identification that contains the candidate's photograph. 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, greencard and national ID. Any candidate who does not provide an acceptable form of identification 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 testing room 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 made available at the test site.
- Candidates are not allowed to bring reference materials or language dictionaries into the test center.
- Candidates are not allowed to bring or use a calculator.
- Candidates are not allowed to bring any type of communication devices (i.e., cell phones, PDAs, Blackberries, etc.) into the test center.
- Scratch paper is not permitted. Candidates may use the margin of the pages, as needed.
- Visitors are not permitted.
- Candidates may be excused to leave the room by the proctor during the exam.
- No food or beverages are allowed.

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

Be Careful in Completing the Answer Sheet

- An example of the multiple-choice answer sheet is included to familiarize candidates with its format.
- Before a candidate begins the exam, the exam 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 site is available. If a candidate desires to take the exam in a language other than the primary language of the test site, 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 or the wrong question. 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. Therefore, it is advisable that candidates 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 their 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 Board 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 testing room. The testing agency will provide the ISACA CISA Certification Board 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

The proctor may dismiss a candidate for any of the following reasons:

- Admission to the test center is unauthorized.
- Candidate creates a disturbance or gives or receives help.
- Candidate attempts to remove test materials or notes from the exam room.
- Candidate impersonates another candidate.
- Candidate brings into the test center reference materials, language dictionaries, a calculator or other items that are not permitted.

Scoring the CISA Exam

The CISA exam consists of 200 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 200-800. 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 ISACA's CISA Certification Board. A candidate receiving a passing score may then apply for certification if all other requirements are met.

The CISA examination contains some questions which are included for research and analysis purpose only. These questions are not separately identified and your final score will be based only on the common scored questions. There are various versions of each exam but only the common questions are scored for your results.

Test scores are not available until approximately eight (8) weeks after the test date. The ISACA CISA Certification Board will mail score reports to the candidates. To ensure the confidentiality of actual scores, test results will not be reported by telephone or fax. Candidates can request an e-mail pass/fail status and score by marking the appropriate box on the CISA exam registration form. This e-mail notification will only be sent to the e-mail address listed in the candidates profile at the time of the initial release of the results. To prevent the e-mail notification from being sent to a spam folder, candidates should add *examregistrant@isaca.org* to their address book, whitelist or safe-senders list.

Candidates will receive a score report containing a subscore for each area. Successful candidates will receive, along with a score report, an application 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 taking either a simple or weighted average of the subscores does not derive the total scaled score.

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, rescoring 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 \$50 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 or description problem 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,

Candidate's Guide to the CISA Exam and Certification

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. The following questions are from past editions of the *CISA Review Questions, Answers & Explanations Manual*, and are examples of the CISA question format. The option in bold is the correct answer.

1. An IS Auditor is assigned to perform a post-implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:
 - A. implemented a specific control during the development of the application system.**
 - B. designed an embedded audit module exclusively for auditing the application system.
 - C. participated as a member of the application system project team, but did not have operational responsibilities.
 - D. provided consulting advice concerning application system best practices.
2. Which of the following **BEST** describes the early stages of an IS audit?
 - A. Observing key organizational facilities
 - B. Assessing the IS environment
 - C. Understanding the business process and environment applicable to the review**
 - D. Reviewing prior IS audit reports
3. When conducting a review of business process reengineering, an IS auditor found that a key preventive control had been removed. The IS auditor should:
 - A. inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.**
 - B. determine if a detective control has replaced the preventive control during the process and, if it has, not report the removal of the preventive control.
 - C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.
 - D. develop a continuous audit approach to monitor the effects of the removal of the previous control.
4. An IS auditor is performing a project review to identify whether a new application has met business objectives. Which of the following test reports offers the most assurance that business objectives are met?
 - A. User acceptance**
 - B. Performance
 - C. Sociability
 - D. Penetration
5. Naming conventions for system resources are important for access control because they:
 - A. ensure that resource names are not ambiguous.
 - B. reduce the number of rules required to adequately protect resources.**
 - C. ensure that user access to resources is clearly and uniquely identified.
 - D. ensure that internationally recognized names are used to protect resources.

CISA Exam Terminology

To assist candidates taking the exam with the translation of technical terminology, a list of the most frequently used technical terms in English along with how they will appear on the exam in other languages offered is available on ISACA's web site at www.isaca.org/examterm.

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**

Candidate's Guide to the CISA Exam and Certification

use the CISA designation, until the completed application is received and approved. Once certified, the new CISA will receive a certificate and a copy of the CISA continuing professional education policy. 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 IS operating or programming experience, or one year of financial or operational auditing experience can be substituted for one year of IS auditing, control, assurance or security experience.
- An associate's or bachelor's degree (the equivalent of 60 to 120 completed college semester credit hours) can be substituted for one or two years, respectively, of IS auditing, control, assurance or security experience.
- A bachelor's degree from a university that enforces the ISACA-sponsored Model Curricula can be substituted for one year of IS auditing, control, assurance or security experience. To view a list of these schools, please visit www.isaca.org/modeluniversities. This option cannot be used if three years of substitution have already been claimed from above.
- Each two years of experience as a full-time university instructor in a related field (e.g., computer science, accounting, IS auditing) may be substituted for one year of IS auditing, control, assurance or security 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.

All experience is verified independently with employers via a Verification of Work Experience form.

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 continuing professional education policy requires the attainment of continuing professional education (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 to ISACA International Headquarters in full.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with ISACA's Code of Professional Ethics.

Failure to comply with these general requirements will result in the revocation of an individual's CISA designation.

Revocation of CISA Certification

The CISA Certification Board 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 continuing professional education 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

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.

Candidate's Guide to the CISA Exam and Certification

CISA Task and Knowledge Statements

CONTENT AREA
<p>The IS Audit Process</p> <p>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.</p>
<p>Tasks</p> <p>Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.</p> <p>Plan specific audits to ensure that IT and business systems are protected and controlled.</p> <p>Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.</p> <p>Communicate emerging issues, potential risks and audit results to key stakeholders.</p> <p>Advise on the implementation of risk management and control practices within the organization, while maintaining independence.</p>
<p>Knowledge Statements</p> <p>Knowledge of ISACA IS Auditing Standards, Guidelines and Procedures and the Code of Professional Ethics</p> <p>Knowledge of IS auditing practices and techniques</p> <p>Knowledge of techniques to gather information and preserve evidence (e.g., observation, inquiry, interview, CAATTs and electronic media)</p> <p>Knowledge of the evidence life cycle (e.g., the collection, protection, chain of custody)</p> <p>Knowledge of control objectives and controls related to IS (e.g., COBIT)</p> <p>Knowledge of risk assessment in an audit context</p> <p>Knowledge of audit planning and management techniques</p> <p>Knowledge of reporting and communication techniques (e.g., facilitation, negotiation and conflict resolution)</p> <p>Knowledge of control self-assessment (CSA)</p> <p>Knowledge of continuous audit techniques</p>
<p>IT Governance</p> <p>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.</p>
<p>Tasks</p> <p>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.</p> <p>Evaluate the IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.</p> <p>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.</p> <p>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.</p> <p>Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standard and procedures.</p> <p>Evaluate IT resource investment, use and allocation practices to ensure alignment with the organization's strategies and objectives.</p> <p>Evaluate IT contracting strategies and policies and contract management practices to ensure that they support the organization's strategies and objectives.</p> <p>Evaluate risk management practices to ensure that the organization's IT-related risks are properly managed.</p> <p>Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.</p>

Candidate's Guide to the CISA Exam and Certification

CONTENT AREA
IT Governance (continued)
Knowledge Statements
Knowledge of the purpose of IT strategies, policies, standards and procedures for an organization and the essential elements of each
Knowledge of IT governance frameworks
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)
Knowledge of quality management strategies and policies
Knowledge of organizational structure, roles and responsibilities related to the use and management of IT
Knowledge of generally accepted international IT standards and guidelines
Knowledge of enterprise IT architecture and its implications for setting long-term strategic goals
Knowledge of risk management methodologies and tools
Knowledge of the use of control frameworks (e.g., COBIT, COSO and ISO/IEC 17799)
Knowledge of the use of maturity and process improvement models (e.g., CMM and COBIT)
Knowledge of contracting strategies, processes and contract management practices
Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards and key performance indicators)
Knowledge of relevant legislative and regulatory issues (e.g., privacy, intellectual property and corporate governance requirements)
Knowledge of IT human resources (personnel) management
Knowledge of IT resource investment and allocation practices (e.g., portfolio management return on investment)
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.
Tasks
Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organization's business goals.
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.
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.
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.
Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organization's objectives.
Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.
Perform postimplementation review of systems and/or infrastructure to ensure that they meet the organization's objectives and are subject to effective internal control.
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.
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.
Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organization's policies and procedures.

Candidate's Guide to the CISA Exam and Certification

CONTENT AREA
Systems and Infrastructure Life Cycle Management (continued)
Knowledge Statements
Knowledge of benefits management practice (e.g., feasibility studies and business cases)
Knowledge of project governance mechanisms (e.g., steering committee and project oversight board)
Knowledge of project management practices, tools and control frameworks
Knowledge of risk management practices applied to projects
Knowledge of project success criteria and risks
Knowledge of configuration, change and release management in relation to development and maintenance of systems and/or infrastructure
Knowledge of control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data within IT systems applications
Knowledge of enterprise architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services and n-tier applications)
Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability and gap analysis)
Knowledge of acquisition and contract management processes (e.g., evaluation of vendors, preparation of contracts, vendor management and escrow)
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)
Knowledge of quality assurance methods
Knowledge of the management of testing processes (e.g., test strategies, test plans, test environments, entry and exit criteria)
Knowledge of data conversion tools, techniques and procedures
Knowledge of system and/or infrastructure disposal procedures
Knowledge of software and hardware certification and accreditation practices
Knowledge of postimplementation review objectives and methods (e.g., project closure, benefits realization and performance measurement)
Knowledge of system migration and infrastructure deployment practices
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.
Tasks
Evaluate service-level management practices to ensure that the level of service from internal and external service providers is defined and managed.
Evaluate operations management to ensure that IT support functions effectively meet business needs.
Evaluate data administration practices to ensure the integrity and optimization of databases.
Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives.
Evaluate change, configuration and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented.
Evaluate problem and incident management practices to ensure that incidents, problems and errors are recorded, analyzed and resolved in a timely manner.
Evaluate the functionality of the IT infrastructure (e.g., network components, hardware and system software) to ensure that it supports the organization's objectives.

Candidate's Guide to the CISA Exam and Certification

CONTENT AREA
IT Service Delivery and Support (continued)
Knowledge Statements
Knowledge of service-level management practices
Knowledge of operations management best practices (e.g., workload scheduling, network services management and preventive maintenance)
Knowledge of system performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports and load balancing)
Knowledge of the functionality of hardware and network components (e.g., routers, switches, firewalls and peripherals)
Knowledge of database administration practices
Knowledge of the functionality of system software including operating systems, utilities and database management systems
Knowledge of capacity planning and monitoring techniques
Knowledge of processes for managing scheduled and emergency changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
Knowledge of incident/problem management practices (e.g., help desk, escalation procedures and tracking)
Knowledge of software licensing and inventory practices
Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure and clustering)
Protection of Information Assets
Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.
Tasks
Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.
Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.
Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.
Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.
Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.
Knowledge Statements
Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis and privacy impact assessment)
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)
Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies and identity management)
Knowledge of attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service and spamming)
Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures and emergency incident response teams)
Knowledge of network and Internet security devices, protocols and techniques (e.g., SSL, SET, VPN and NAT)
Knowledge of intrusion detection systems and firewall configuration, implementation, operation and maintenance
Knowledge of encryption algorithm techniques (e.g., AESRSA)
Knowledge of public key infrastructure (PKI) components (e.g., certification authorities and registration authorities) and digital signature techniques

Candidate's Guide to the CISA Exam and Certification

CONTENT AREA
Protection of Information Assets (continued)
Knowledge Statements
Knowledge of virus detection tools and control techniques
Knowledge of security testing and assessment tools (e.g., penetration testing and vulnerability scanning)
Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems and water sensors)
Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks and tokens)
Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data)
Knowledge of voice communications security (e.g., voiceover IP)
Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., PDAs, USB devices and Bluetooth devices)
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.
Tasks
Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing.
Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.
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
Knowledge of data backup, storage, maintenance, retention and restoration processes and practices
Knowledge of regulatory, legal, contractual and insurance issues related to business continuity and disaster recovery
Knowledge of business impact analysis (BIA)
Knowledge of the development and maintenance of the business continuity and disaster recovery plans
Knowledge of business continuity and disaster recovery testing approaches and methods
Knowledge of human resources management practices as related to business continuity and disaster recovery (e.g., evacuation planning and response teams)
Knowledge of processes used to invoke the business continuity and disaster recovery plans
Knowledge of types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites and cold sites)

Candidate's Guide to the CISA Exam and Certification

THE CISA EXAMINATION AND COBIT

COBIT 4.1 is an initiative conducted by the IT Governance Institute. COBIT has been developed as a generally applicable and accepted framework for good IT security and control practices that provide a reference for management, users, and IS audit, control and security practitioners. COBIT is based on ITGI's control objectives, enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for application to organizationwide information systems.

COBIT also supports a generic IT assurance/audit process which can be summarized as:

- Obtaining an understanding of business requirements, related risks and relevant control measures
- Evaluating the appropriateness of stated controls
- Assessing compliance by testing whether the stated controls are working: as prescribed, consistently and continuously
- Substantiating the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources

Although knowledge of COBIT is not specifically tested on the CISA examination, the COBIT control objectives or processes reflect the tasks identified in the CISA job practice. As such, a thorough review of COBIT is recommended for candidate preparation for the CISA examination. To focus a candidate's attention on the specific COBIT processes that relate to CISA practice analysis tasks, the following table has been provided to aid in a candidate's exam preparation.

Domain	Process
Plan and Organise	PO1 Define a strategic IT plan. PO2 Define the information architecture. PO3 Determine technological direction. PO4 Define the IT processes, organisation and relationships. PO5 Manage the IT investment. PO6 Communicate management aims and direction. PO7 Manage IT human resources. PO8 Manage quality. PO9 Assess and manage IT risks. PO10 Manage projects.
Acquire and Implement	AI1 Identify automated solutions. AI2 Acquire and maintain application software. AI3 Acquire and maintain technology infrastructure. AI4 Ensure operation and use. AI5 Procure IT resources. AI6 Manage changes. AI7 Install and accredit solutions and changes.
Deliver and Support	DS1 Define and manage service levels. DS2 Manage third-party services. DS3 Manage performance and capacity. DS4 Ensure continuous service. DS5 Ensure systems security. DS6 Identify and allocate costs. DS7 Educate and train users. DS8 Manage service desk and Incidents. DS9 Manage the configuration. DS10 Manage problems. DS11 Manage data. DS12 Manage the physical environment. DS13 Manage operations.
Monitor and Evaluate	ME1 Monitor and evaluate IT performance. ME2 Monitor and evaluate internal control. ME3 Ensure compliance with external requirements. ME4 Provide IT governance.

Candidate's Guide to the CISA Exam and Certification

Suggested Resources for Further Study

The following are references recommended for further study in preparation for the exam. A more comprehensive list can be found in the *CISA Review Manual 2008*.

Content Area 1—The IS Audit Process

International Federation of Accountants, *Handbook of International Auditing, Assurance, and Ethics Pronouncements*, 2003, www.ifac.org

ISACA, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals, USA, 2007*, www.isaca.org/standards

IT Governance Institute, *Control Objectives for Information and related Technology (COBIT) 4.1*, USA, 2007

IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, USA, 2006, www.isaca.org/sox

Parker, Xenia Ley; *Information Technology Audits*, 2007 Edition, CCH, USA, 2007

Sarva, Srinivas; "Continuous Auditing Through Leveraging Technology," *Information Systems Control Journal*, vol. 2, 2006, p. 47-50

Senft, Sandra; Daniel P. Manson; Carol Gonzales; Frederick Gallegos; *Information Technology Control and Audit, 2nd Edition*, Auerbach, USA, 2004

Solís Montes, Gustavo Adolfo; *Reingeniería de la Auditoría Informática, Editorial Trillas* (Spanish only), Mexico, 2002

Van Grembergen, Wim; Steven De Haes; Jan Moons; "IT Governance: Linking Business Goals to IT Goals and COBIT Processes," *Information Systems Control Journal*, vol. 4, 2005, p. 18-22

Content Area 2—IT Governance

Brothby, W. Krag; IT Governance Institute; *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, IT Governance Institute, USA, 2006

De Haes, Steven; David Gilmore; Wim Van Grembergen; Gary Hardy; Alan Simmons; Paul A. Williams; Lighthouse Global; ITGI; *IT Governance Domain Practices and Competencies Series*, IT Governance Institute, USA, 2005

Finne, Thomas; "Audit and Assurance of Information Systems and Business Processes: A Foundation for Providing Sound Governance Decision Making," *Information Systems Control Journal*, vol. 1, 2006, p. 40-42

Grembergen, Wim Van; Steven De Haes; "COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade," *Information Systems Control Journal*, vol. 6, 2005, p. 54-56

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

IT Governance Institute, COBIT 4.1, *Control Objectives*, PO1, PO4, PO5, PO6, PO7, PO8, PO9, PO10, AI6, DS1, DS2, DS6, DS7, DS11, ME, ME3, AI2, USA, 2007

Simmonds, Alan; David Gilmore; Lighthouse Global; IT Governance Institute; *Governance of Outsourcing*, IT Governance Institute, USA, 2005

Note: Publications in bold are stocked in the ISACA Bookstore. *Information Systems Control Journal* articles are available at www.isaca.org/archives. The articles are available online to ISACA members only during their first year of release, and then are opened to the public. All referenced *Journal* articles are available on the CISA Practice Question Database v8.

Candidate's Guide to the CISA Exam and Certification

Content Area 3—Systems & Infrastructure Lifecycle Management

Doss, George M.; Michael Wallace; Larry Webber; *IS Project Management Handbook 2006 Edition*, Aspen Publishers Inc., USA, 2006

International Organization for Standardization and the International Electrotechnical Commission, "Information Technology—Software Process Assessment—Part 5," ISO/IEC TR 15504-5: 1999, UK, 2000, www.isospice.com

Information Processing Limited, "Software Testing and Software Development Lifecycles," www.ipl.com/pdf/p0821.pdf

IT Governance Institute, *Measuring and Demonstrating the Value of IT*, USA, 2005

Maizlish, Bryan; Robert Handler; *IT Portfolio Management Step-by-Step: Unlocking the Business Value of Technology*, John Wiley & Sons, USA, 2005

Malik, Shadan; *Enterprise Dashboards: Design and Best Practices for IT*, John Wiley & Sons, USA, 2005

Content Area 4—IT Service Delivery & Support

Braag, Roberta; Mark Rhode-Ousley; Keith Strassburg; *The Complete Reference Network Security*, McGraw Hill, USA, 2003

Dimitriadis, Christos K.; "Improving Security Management for Mobile Operators," *Information Systems Control Journal*, vol. 4, 2006, p. 28-32

Du, Hui; Chen Zhang; "Risks and Risk Control of Wi-Fi Network Systems," *Information Systems Control Journal*, vol. 4, 2006, p. 38-44

Hoelsing, Michael T.; Vasant Raval; "Using Wireless Network Audit Techniques," *Information Systems Control Journal*, vol. 3, 2004, p. 39-42

Merkow, Mark S.; James Breithaupt; *The Complete Guide to Security*, American Management Association, USA, 2000

National Institute of Standards and Technology, "Security Considerations for Voice Over IP Systems," USA, 2005

Schneier, Bruce; *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, USA, 2004

Tanenbaum, Andrew S.; *Modern Operating Systems, 2nd Edition*, USA, 2001

Content Area 5—Protection of Information Assets

Coderre, David G.; *Fraud Detection: A Revealing Look at Fraud, 2nd Edition*, Ekaros Analytical Inc., Canada, 2004

Gallegos, Frederick; "Computer Forensics: An Overview," *Information Systems Control Journal*, vol. 6, 2005, p. 13-16

Harris, Shon; Allen Harper; Chris Eagle; Jonathan Ness; Michael Lester; *Gray Hat Hacking*, McGraw Hill, USA, 2005

International Organisation for Standardisation; "Information Technology—Code of Practice for Information Security Management," ISO/IEC 17799:2000, UK, 2000

Kairab, Sudhanshu; *A Practical Guide to Security Assessments*, Auerbach Publications, USA, 2004

Note: Publications in bold are stocked in the ISACA Bookstore. *Information Systems Control Journal* articles are available at www.isaca.org/archives. The articles are available online to ISACA members only during their first year of release, and then are opened to the public. All referenced *Journal* articles are available on the CISA Practice Question Database v8.

Candidate's Guide to the CISA Exam and Certification

McClure, Stuart; Joel Sambray; George Kurtz; *Hacking Exposed, 5th Edition*, McGraw Hill, USA, 2005

McKemmish, D. Rodney; "Computer and Intrusion Forensics," ArTech House Inc., USA, 2003

Mitnick, Kevin D.; William L. Simon; *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Wiley Publishing, Inc., USA, 2005

Peltier, Thomas R.; *Information Security Risk Analysis, 2nd Edition*, Auerbach Publications, USA, 2005

Pironti, John P.; "Key Elements of a Threat and Vulnerability Management Program," *Information Systems Control Journal*, vol. 3, 2006, p. 52-56

Schneier, Bruce; *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, USA, 2004

Stamp, Mark; *Information Security: Principles and Practice*, John Wiley & Sons, USA, 2005

Stanley, Richard A.; *Managing Risk in the Wireless Environment: Security, Audit and Control Issues*, ISACA, USA, 2005

Tudor, Jan Killmeyer; *Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition*, Auerbach Publications, USA, 2005

Content Area 6—Business Continuity & Disaster Recovery

Castella, Stephen; "Foundations for Successful BCP in Your IT Department," Contingency Planning & Management web site, 2003, www.contingencyplanning.com/Tools/BCPHandbook/BCP102.asp

Edwards Information, LLC; *Disaster Recovery Directory, 15th Edition*, Edwards Information, USA, 2006

Fulmer, Kenneth L.; *Business Continuity Planning: A Step-by-Step Guide with Planning Forms on CD-ROM*, Rothstein Associates Inc., USA, 2005

Goggins, Kelley; "Contingency Planning 101," Contingency Planning & Management, 2003, www.contingencyplanning.com/Tools

ISACA; *Cybercrime: Incident Response & Digital Forensics*, USA, 2005

Raval, Vasant; Ashok Fichdia; *Risks, Controls, and Security: Concepts and Applications*, John Wiley & Sons, USA, 2007, Chapter 6: System Availability and Business Continuity

Shimonski, Robert J.; "Your Quick Guide to Common Attacks," Windows Security, 20 May 2003, www.windowsecurity.com/articles/Common_Attacks.html

Toigo, Jon William; *Disaster Recovery Planning: Preparing for the Unthinkable, 3rd Edition*, Prentice Hall, USA, 2003

Von Roessing, Rolf; *Auditing Business Continuity: Global Best Practices*, Rothstein Associates, USA, 2002

Wells, April; Charlyne Walker; Timothy Walker; *Disaster Recovery: Principles and Practices*, USA, Pearson-Prentice Hall, 2007.

Note: Publications in bold are stocked in the ISACA Bookstore. *Information Systems Control Journal* articles are available at www.isaca.org/archives. The articles are available online to ISACA members only during their first year of release, and then are opened to the public. All referenced *Journal* articles are available on the CISA Practice Question Database v8.

Candidate's Guide to the CISA Exam and Certification

List of Acronyms

The CISA candidate should be familiar with the following list of acronyms. These acronyms are the only stand-alone abbreviations used in exam questions.

ASCII	American Standard Code for Information Interchange	IT	Information technology
Bit	Binary digit	LAN	Local area network
CASE	Computer-aided system engineering	PBX	Private branch (business) exchange
CCTV	Closed-circuit television	PC	Personal computer/microcomputer
CPU	Central processing unit	PCR	Program change request
DBA	Database administrator	PDA	Personal digital assistant
DBMS	Database management system	PERT	Program Evaluation Review Technique
EDI	Electronic data interchange	PIN	Personal identification number
FTP	File Transfer Protocol	PKI	Public key infrastructure
HTTP	Hypertext Transmission Protocol	RAID	Redundant Array of Inexpensive Disks
HTTPS	Secured Hypertext Transmission Protocol	RFID	Radio frequency identification
ID	Identification	SDLC	System development life cycle
IDS	Intrusion detection system	SSL	Secure Sockets Layer
IP	Internet protocol	TCP	Transmission Control Protocol
IS	Information systems	UPS	Uninterruptible power supply
ISO	International Organization for Standardization	VoIP	Voice-over Internet Protocol
		WAN	Wide area network

In addition to the aforementioned acronyms, candidates may also wish to become familiar with the following additional acronyms. Should any of these abbreviations be used in exam questions, their meanings would be included when the acronym appears.

4GL	Fourth-generation language	BOM	Bill of materials
ACID	Atomicity, consistency, isolation and durability	BOMP	Bill of materials processor
ACL	Access control list	BPR	Business process reengineering
AES	Advanced Encryption Standard	BRP	Business recovery (or resumption) plan
AH	Authentication header	BSC	Balanced scorecard
AI	Artificial intelligence	CA	Certificate authority
AICPA	American Institute of Certified Public Accountants	CAAT	Computer-assisted audit technique
ALE	Annual loss expectancy	CAD	Computer-assisted design
ALU	Arithmetic-logic unit	CAE	Computer-assisted engineering
ANSI	American National Standards Institute	CAM	Computer-aided manufacturing
API	Application programming interface	CASE	Computer-aided software engineering
ARP	Address Resolution Protocol	CCK	Complimentary Code Keying
ASIC	Application-specific integrated circuit	CCM	Constructive Cost Model
ATDM	Asynchronous time division multiplexing	CD	Compact disk
ATM	Asynchronous Transfer Mode or automated teller machine	CD-R	Compact disk-recordable
B-to-B	Business-to-business	CD-RW	Compact disk-rewritable
B-to-C	Business-to-consumer	CDDF	Call Data Distribution Function
B-to-E	Business-to-employee	CDPD	Cellular Digital Packet Data
B-to-G	Business-to-government	CEO	Chief executive officer
BCI	Business Continuity Institute	CERT	Computer emergency response team
BCM	Business continuity management	CGI	Common gateway interface
BCP	Business continuity planning	CIAC	Computer Incident Advisory Capability
BI	Business intelligence	CICA	Canadian Institute of Chartered Accountants
BIA	Business impact analysis	CIM	Computer-integrated manufacturing
BIMS	Biometric Information Management and Security	CIO	Chief information officer
BIOS	Basic Input/Output System	CIS	Continuous and intermittent simulation
BIS	Bank for International Settlements	CISO	Chief information security officer
BLP	Bypass label process	CMDB	Configuration management database
BNS	Backbone network services	CMM	Capability Maturity Model
		CMMI	Capability Maturity Model Integration

Candidate's Guide to the CISA Exam and Certification

CNC	Computerized Numeric Control	EAI	Enterprise application integration
COBIT	<i>Control Objectives for Information and related Technology</i>	EAM	Embedded audit module
COCOMO2	Constructive Cost Model	EAP	Extensible Authentication Protocol
CODASYL	Conference on Data Systems Language	EBCDIC	Extended Binary-coded for Decimal Interchange Code
COM	Component Object Model	EC	Electronic commerce
COM/DCOM	Component Object Model/Distributed Component Object Model	ECC	Elliptical curve cryptography
COOP	Continuity of operations plan	EDFA	Enterprise data flow architecture
CORBA	Common Object Request Broker Architecture	EER	Equal-error rate
CoS	Class-of-service	EFT	Electronic funds transfer
COSO	Committee of Sponsoring Organizations of the Treadway Commission	EIGRP	Enhanced Interior Gateway Routing Protocol
CPM	Critical Path Methodology	EJB	Enterprise java beans
CPO	Chief privacy officer	EMI	Electromagnetic interference
CPS	Certification practice statement	EMRT	Emergency response time
CRC	Cyclic redundancy check	ERD	Entity relationship diagram
CRL	Certificate revocation list	ERP	Enterprise resource planning
CRM	Customer relationship management	ESP	Encapsulating security payload
CSA	Control self-assessment	EVA	Earned value analysis
CSF	Critical success factor	FAR	False-acceptance rate
CSIRT	Computer security incident response team	FAT	File allocation table
CSMA/CD	Carrier-sense Multiple Access/Collision Detection	FC	Fibre channels
CSO	Chief security officer	FDDI	Fiber-Distributed Data Interface
CSU-DSU	Channel service unit/digital service unit	FDM	Frequency division multiplexing
DAC	Discretionary access controls	FEA	Federal enterprise architecture
DASD	Direct access storage device	FEMA	Federal Emergency Management Association (USA)
DAT	Digital audio tape	FER	Failure-to-enroll rate
DCE	Data communications equipment	FERC	Federal Energy Regulatory Commission (USA)
DCE	Distributed computing environment	FFIEC	Federal Financial Institutions Examination Council (USA)
DCOM	Distributed Component Object Model (Microsoft)	FFT	Fast Fourier Transform
DCT	Discrete Cosine Transform	FHSS	Frequency-hopping spread spectrum
DD/DS	Data dictionary/directory system	FIPS	Federal Information Processing Standards
DDL	Data Definition Language	FP	Function point
DDN	Digital Divide Network	FPA	Function point analysis
DDoS	Distributed denial of service	FRAD	Frame relay assembler/disassembler
DECT	Digital Enhanced Cordless Telecommunications	FRB	Federal Reserve Board (USA)
DES	Data Encryption Standard	FRR	False-rejection rate
DFD	Data flow diagram	GAS	Generalized audit software
DHCP	Dynamic Host Configuration Protocol	GB	Gigabyte
DID	Direct inward dial	GID	Group ID
DIP	Document image processing	GIS	Geographic information systems
DLL	Dynamic link library	GPS	Global position system
DMS	Disk management system	GSM	Global system for mobile communications
DMZ	Demilitarized zone	GUI	Graphical user interface
DNS	Domain name server	HA	High availability
DoS	Denial of service	HD-DVD	High definition/high density-digital video disc
DOSD	Data-oriented system development	HDLC	High-level data link control
DRII	Disaster Recovery Institute International	HIPAA	Health Insurance Portability and Accountability Act (USA)
DRP	Disaster recovery planning	HIPO	Hierarchy input-process-output
DSL	Digital subscriber lines	HTML	Hypertext Markup Language
DSS	Decision support systems	HW/SW	Hardware/software
DSSS	Direct-sequence spread spectrum (DSSS)	I/O	Input/output
DTE	Data terminal equipment	I&A	Identification and authentication
DTR	Data terminal ready	ICMP	Internet Control Message Protocol
DVD	Digital video disc	ICT	Information and communication technologies
DVD-HD	Digital video disc-high definition/high density	IDE	Integrated development environment
DW	Data warehouse	IDEF1X	Integration Definition for Information Modeling
EA	Enterprise architecture	IETF	Internet Engineering Task Force
EAC	Estimates at completion	IPF	Information processing facility

Candidate's Guide to the CISA Exam and Certification

IPL	Initial program load	NTP	Network Time Protocol
IPMA	International Project Management Association	OBS	Object Breakdown Structure
IPRs	Intellectual property rights	OCSP	Online Certificate Status Protocol
IPS	Intrusion prevention system	OECD	Organization for Economic Cooperation and Development
IPSec	IP Security	OEP	Occupant emergency plan
IPX	Internetwork Packet Exchange	OFDM	Orthogonal frequency division multiplexing
IR	Incident response	OLAP	Online analytical processing
IR	Infrared	OO	Object-oriented
IRC	Internet relay chat	OOSD	Object-oriented system development
IrDA	Infrared Data Association	ORB	Object request broker (ORB)
IRM	Incident response management	OS	Operating system
IS/ORP	IS disaster recovery planning	OSI	Open Systems Interconnection
ISAKMP/ Oakley	Internet Security Association and Key Management Protocol/Oakley	OSPF	Open Shortest Path First
ISAM	Indexed Sequential Access Method	PAD	Packet assembler/disassembler
ISDN	Integrated services digital network	PAN	Personal area network
ISP	Internet service provider	PBX	Private branch exchange
ITF	Integrated test facility	PDCA	Plan-Do-Check-Act
ITGI	IT Governance Institute	PDN	Public data network
ITIL	Information Technology Infrastructure Library	PER	Package-enabled reengineering
ITSM	IT service management	PHY	Physical layer
ITT	Invitation to tender	PICS	Platform for Internet content selection
ITU	International Telecommunications Union	PID	Process ID
JIT	Just in time	PID	Project Initiation Document
Kb	Kilobit	PMBOK	Project Management Body of Knowledge
KB	Kilobyte	PMI	Project Management Institute
KB	Knowledge base	POC	Proof of concept
KDSI	Thousand delivered source instructions	POP	Proof of possession
KGI	Key goal indicator	POS	Point of sale or Point-of-sale systems
KLOC	Kilo lines of code	POTS	Plain old telephone service
KPI	Key performance indicator	PPP	Point-to-point Protocol
L2TP	Layer 2 Tunneling Protocol	PPPoE	Point-to-point Protocol Over Ethernet
LCP	Link Control Protocol	PPTP	Point-to-Point Tunneling Protocol
M&A	Mergers and acquisition	PR	Public relations
MAC	Mandatory Access Control	PRD	Project request document
MAC address	Media Access Control address	PRINCE2	Projects in Controlled Environments 2
MAN	Metropolitan area network	PROM	Programmable Read-Only Memory
MAP	Manufacturing accounting and production	PSTN	Public switched telephone network
MIS	Management information system	PVC	Permanent virtual circuit
MODEM	Modulator/demodulator	QA	Quality assurance
MOS	Maintenance out of service	QAT	Quality assurance testing
MPLS	Multiprotocol label switching	RA	Registration authority
MRP	Manufacturing resources planning	RAD	Rapid application development
MSAUs	Multistation access units	RADIUS	Remote Access Dial-in User Service
MTBF	Mean time between failures	RAID	Redundant Array of Inexpensive Disks
MTS	Microsoft's Transaction Server	RAM	Random access memory
MTTR	Mean time to repair	RAS	Remote access service
NAP	Network access point	RBAC	Role-based access control
NAS	Network access server or Network attached storage	RDBMS	Relational database management system
NAT	Network address translation	RF	Radio frequency
NCP	Network Control Protocol	RFI	Request for information
NDA	Nondisclosure agreement	RFP	Request for proposal
NFPA	National Fire Protection Agency (USA)	RIP	Routing Information Protocol
NFS	Network file system	RMI	Remote method invocation
NIC	Network interface card	ROI	Return on investment
NIST	National Institute of Standards and Technology (USA)	ROLAP	Relational online analytical processing
NNTP	Network News Transfer Protocol	ROM	Read-only memory
NSP	Name Server Protocol or Network service provider	RPC	Remote procedure call
NT	New technology	RPO	Recovery point objective
NTFS	NT file system	RST	Reset

Candidate's Guide to the CISA Exam and Certification

RTO	Recovery time objective	TR	Technical report
RW	Rewritable	UAT	User acceptance testing
S/HTTP	Secure Hypertext Transfer Protocol	UBE	Unsolicited bulk e-mail
S/MIME	Secure Multipurpose Internet Mail Extensions	UDDI	Description, discovery and integration
SA	Security Association	UDP	User Datagram Protocol
SAN	Storage area network	UID	User ID
SANS	The SANS Institute	UML	Unified Modeling Language
SAS	Statement on Auditing Standards	URI	Uniform resource identifier
SBC	Session border controller	URL	Universal resource locator
SCADA	Supervisory Control and Data Acquisition	URN	Uniform resource name
SCARF	Systems Control Audit Review File	USB	Universal Serial Bus
SCARF/EAM	Systems Control Audit Review File and Embedded Audit Modules	VLAN	Virtual local area network
SCM	Supply Chain Management	VoIP	Voice-Over IP
SCOR	Supply Chain Operations Reference	VPN	Virtual private network
SD/MMC	Secure digital multimedia card	WAP	Wireless Application Protocol
SDLC	System development life cycle	WBS	Work breakdown structure
SDO	Service delivery objective	WEP	Wired Equivalent Privacy
SEC	Securities and Exchange Commission (USA)	WLAN	Wireless local area network
SET	Secure electronic transactions	WML	Wireless Markup Language
SLA	Service level agreement	WORM	Write-once and read many
SLIP	Serial Line Internet Protocol	WP	Work packages
SLM	Service level management	WPA	Wi-Fi Protected Access
SLOC	Source lines of code	WPAN	Wireless personal area network
SMART	Specific, measurable, achievable, relevant, time-bound	WSDL	Web Services Description Language
SME	Subject matter expert	WWAN	Wireless wide area network
SMF	System management facility	WWW	World Wide Web
SMTP	Simple Mail Transport Protocol	X-to-X	Exchange-to-Exchange
SNA	Systems network architecture	XBRL	Extensible Business Reporting Language
SNMP	Simple Network Management Protocol	XML	Extensible Markup Language
SO	Security officer	Xquery	XML query
SOA	Service-oriented architecture	XSL	Extensible Stylesheet Language
SOAP	Simple Object Access Protocol		
SOHO	Small office-home office		
SPI	Security parameter index		
SPICE	Software Process Improvement and Capability Determination		
SPOC	Single point of contact		
SPOOL	Simultaneous peripheral operations online		
SQL	Structured Query Language		
SSH	Secure Shell		
SSID	Set services identifiers		
SSO	Single sign-on		
SVC	Switched virtual circuits		
SYSGEN	System generation		
TACACS	Terminal Access Control Access Control System		
TCO	Total cost of ownership		
TCP/IP	Transmission Control Protocol/Internet Protocol		
TCP/UDP	Transmission Control Protocol/User Datagram Protocol		
TDM	Time-division multiplexing		
TELNET	Teletype network		
TES	Terminal emulation software		
TFTP	Trivial File Transport Protocol		
TKIP	Temporal Key Integrity Protocol		
TLS	Transport layer security		
TMS	Tape management system		
TP monitors	Transaction processing (TP) monitors		
TQM	Total quality management		

Candidate's Guide to the CISA Exam and Certification

Sample Admission Ticket

The following is an example of the admission ticket that candidates will receive approximately two to three weeks prior to the CISA exam date.

CISA EXAM ADMISSION TICKET

[Date]

[Exam Registrant Address]

[Exam Registrant Name]:

On behalf of ISACA we want to thank you for registering for the ISACA [Month Year] Certified Information Systems Auditor (CISA) exam. Your **Identification Number** is [NNNNNNNN]. You are scheduled for the [Language Name] language exam on [Exam Day and Date]. On the day of the exam, report to the test site no later than [Report Time]. Exam instructions will begin at [Instruction Time]. The Exam will start at [Start Time] and end at [End Time]. **The start time may vary slightly due to the onsite registration process.**

Test Site Number: [Site Number]
[Test Site Location and Address]

Special exam accommodations arranged for you include: <none>.

NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS. Any candidate who arrives after the oral instructions have begun **will not be allowed** to sit for the exam and will forfeit their registration fee. To ensure that you arrive in plenty of time for the exam, we recommend that you become familiar with the exact location and the best travel route to your exam site prior to the date of the exam. Test center phone numbers and web site references have been provided (when available) to assist you in obtaining directions to the facility.

YOU MUST bring your exam admission ticket (hard copy or ISACA e-Ticket), several sharpened No. 2 or HB pencils, an eraser, and an acceptable form of **photo identification** such as a driver's license, passport or government ID to the test site. **This ID must be a current and original government issued identification that contains both your name as it appears on the admission ticket and your photograph.** Any candidate who does not provide an acceptable form of identification will not be allowed to sit for the exam and will forfeit their registration fee. Candidates are not allowed to bring any type of communication device (i.e., cell phone, PDA, Blackberry, etc.) into the test center. Discovery of such devices may result in disqualification and/or the device being confiscated. For further details regarding what personal belongings can and cannot be brought with you to the test site, please visit <http://www.isaca.org/cisabelongings>.

Please review the admission ticket details carefully. If you find any of the information on the exam admission ticket is incorrect, please contact the ISACA certification department at +1.847.660.5660 or via email at examREGISTRANT@isaca.org with the specific problems.

-----ISACA Change Form-----

DO NOT return this part of the form if there are NO changes to be recorded. Please print clearly any change or correction to your name, address or ID# below and return this part of the form to your exam proctor when instructed to do so.

[Exam Date and Test Site Number]
ID# [NNNNNNNN]
[Exam Registrant Address]

Candidate's Guide to the CISA Exam and Certification

(Side 2)

YOUR SIGNATURE/SEAL REQUIRED HERE:

- 81 A B C D
- 82 A B C D
- 83 A B C D
- 84 A B C D
- 85 A B C D
- 86 A B C D
- 87 A B C D
- 88 A B C D
- 89 A B C D
- 90 A B C D
- 91 A B C D
- 92 A B C D
- 93 A B C D
- 94 A B C D
- 95 A B C D
- 96 A B C D
- 97 A B C D
- 98 A B C D
- 99 A B C D
- 100 A B C D
- 101 A B C D
- 102 A B C D
- 103 A B C D
- 104 A B C D
- 105 A B C D
- 106 A B C D
- 107 A B C D
- 108 A B C D
- 109 A B C D
- 110 A B C D
- 111 A B C D
- 112 A B C D
- 113 A B C D
- 114 A B C D
- 115 A B C D
- 116 A B C D
- 117 A B C D
- 118 A B C D
- 119 A B C D
- 120 A B C D
- 121 A B C D
- 122 A B C D
- 123 A B C D
- 124 A B C D
- 125 A B C D
- 126 A B C D
- 127 A B C D
- 128 A B C D
- 129 A B C D
- 130 A B C D
- 131 A B C D
- 132 A B C D
- 133 A B C D
- 134 A B C D
- 135 A B C D
- 136 A B C D
- 137 A B C D
- 138 A B C D
- 139 A B C D
- 140 A B C D
- 141 A B C D
- 142 A B C D
- 143 A B C D
- 144 A B C D
- 145 A B C D
- 146 A B C D
- 147 A B C D
- 148 A B C D
- 149 A B C D
- 150 A B C D
- 151 A B C D
- 152 A B C D
- 153 A B C D
- 154 A B C D
- 155 A B C D
- 156 A B C D
- 157 A B C D
- 158 A B C D
- 159 A B C D
- 160 A B C D
- 161 A B C D
- 162 A B C D
- 163 A B C D
- 164 A B C D
- 165 A B C D
- 166 A B C D
- 167 A B C D
- 168 A B C D
- 169 A B C D
- 170 A B C D
- 171 A B C D
- 172 A B C D
- 173 A B C D
- 174 A B C D
- 175 A B C D
- 176 A B C D
- 177 A B C D
- 178 A B C D
- 179 A B C D
- 180 A B C D
- 181 A B C D
- 182 A B C D
- 183 A B C D
- 184 A B C D
- 185 A B C D
- 186 A B C D
- 187 A B C D
- 188 A B C D
- 189 A B C D
- 190 A B C D
- 191 A B C D
- 192 A B C D
- 193 A B C D
- 194 A B C D
- 195 A B C D
- 196 A B C D
- 197 A B C D
- 198 A B C D
- 199 A B C D
- 200 A B C D

Mark Review® by NCS EM-239649-1565321

HF04

Printed in U.S.A.

© Copyright 2001 by National Computer Systems, Inc. All rights reserved.

SAMPLE

Chicago is:

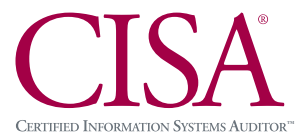
1. a country
2. a mountain
3. an island
4. a city

WRONG WRONG

WRONG WRONG

WRONG RIGHT

WRONG RIGHT



3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

E-mail: *certification@isaca.org*

Web site: *www.isaca.org*