

CISA[®]

CERTIFIED INFORMATION SYSTEMS AUDITOR™

2006 Candidate's Guide to the CISA Exam

Exam Date: 10 June 2006

Early Registration Deadline: 8 February 2006

Final Registration Deadline: 5 April 2006

Exam Date: 9 December 2006

Early Registration Deadline: 16 August 2006

Final Registration Deadline: 29 September 2006

Table of Contents

Introduction	.1
Benefits of Becoming a CISA	.1
CISA Program Receives ANSI Accreditation	.1
The CISA Exam	.2
Study Aids for the CISA Exam	.3
Administration of the CISA Exam	.4
Scoring the CISA Exam	.5
Types of Questions on the CISA Exam	.6
CISA Exam Terminology	.7
Application for CISA Certification	.7
Requirements for Initial CISA Certification	.7
Requirements for Maintaining CISA Certification	.8
Revocation of CISA Certification	.8
ISACA Code of Professional Ethics	.8
Content of the CISA Exam	.9
The CISA Exam and COBIT	.15
Reference Materials	.25
List of Acronyms	.42
Sample Admission Ticket	.44
Sample Answer Sheet	.45

Candidate's Guide to the CISA Exam

ISACA

ISACA is a leading global professional organization representing individuals in more than 140 countries and comprising all levels of information technology—executive, senior management, middle management and practitioner. The association is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards worldwide. Its strategic alliances with other organizations in the financial, accounting and IT professions ensure an unparalleled level of integration and commitment by business process owners.

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 the use of this guide or any other association publication will assure candidates of passing the CISA exam.

Disclosure

Copyright © 2006 by ISACA. Reproduction or storage in any form for any purpose is not permitted without ISACA 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: certification@isaca.org
Web site: www.isaca.org

ISBN 1-933284-35-8

Candidate's Guide to the CISA Exam

Printed in the United States of America.

Candidate's Guide to the CISA Exam

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

Today, 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.

Benefits of Becoming a CISA

Being recognized as a CISA brings with it a great number of professional and organizational benefits. Successful achievement demonstrates and attests to an individual's information systems audit, control and security expertise and indicates a desire to serve an organization with distinction. This expertise is extremely valuable given the changing nature of information technology. With these changes comes a need for organizations to employ certified professionals who are able to apply the most effective information systems audit, control and security practices, and who have an awareness of the unique requirements particular to information technology environments. Those who become CISAs join other recognized professionals worldwide who have earned this highly sought-after professional designation.

A growing number of organizations are requiring or recommending that employees become certified. In a recent benchmarking survey conducted by ISACA, more than half of the individuals surveyed responded that it is their department policy to recognize individuals who obtain a professional certification. This included a monetary bonus, promotion within 12 months or some other type of reward. Many employers require the achievement and maintenance of the CISA designation as a strong factor for employment and/or advanced promotion because it assures that staff is able to apply state-of-the-art information systems audit, control and security practices.

CISA Program Accredited 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 and CISM's will continue to present themselves around the world.

Candidate's Guide to the CISA Exam

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 process and content areas (see the Content of the CISA Exam section on page 9), 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, administered annually in June and December during a four-hour session. Candidates may take the exam in Dutch, English, French, German, Hebrew, Italian, Japanese, Korean, simplified Mandarin Chinese, Spanish and traditional Mandarin Chinese for the June administration and English, French, German, Japanese, Korean Simplified Mandarin Chinese, Spanish, and traditional Mandarin Chinese for the December administration.

Refund and Deferral of Fees

Refund: Candidates unable to take the exam are eligible for a refund of registration fees, less a US \$100 processing fee, if such a request is received in writing on or before 14 April 2006 for the June exam and 13 October 2006 for the December exam. All requests after the respective dates will be denied.

Deferral: Candidates unable to take the exam can request a deferral of their registration fees to the next exam date. For the June 2006 exam, deferral requests received on or before 1 May 2006 will be charged a \$50 processing fee. From 2 May 2006 through 2 June 2006, a processing fee of \$100 will be charged. Deferral requests for the June exam will not be accepted after 2 June 2006.

For the December 2006 exam, deferral requests received on or before 1 November 2006 will be charged a \$50 processing fee. From 2 November 2006 through 1 December 2006, a processing fee of \$100 will be charged. Deferral requests for the December exam will not be accepted after 1 December 2006.

To request a deferral, please visit www.isaca.org/examdefer. NO REFUNDS OR EXCHANGES WILL BE GIVEN FOR STUDY AIDS, ASSOCIATED TAXES, SHIPPING AND HANDLING CHARGES OR MEMBERSHIP FEES.

Candidate's Guide to the CISA Exam

Study Aids 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/cisaexam for more details).

- The *Candidate's Guide to the CISA Exam* is supplied to individuals upon receipt of the CISA exam registration form and payment. This guide provides a detailed outline (task and knowledge statements) of the six content areas covered on the exam. It also contains exam administration information, examples of question types, certification and recertification requirements, a suggested list of reference materials, a list of acronyms commonly used on the exam, and a sample copy of an admission ticket and exam answer sheet.
- The *CISA Review Manual 2006* has been updated to reflect the new CISA job practice and has been enhanced with new topics and issues to reflect changing industry principles and practices. It is a comprehensive study guide that assists individuals in preparing for the CISA exam. The manual features detailed descriptions of the current tasks performed by IS auditors and the knowledge required to plan, manage and perform IS audits. The structure of the manual includes job content areas and related tasks that an IS auditor should know, including detailed explanations of relevant principles and practices. The manual also provides definitions, CISA exam practice questions similar in content to what has previously appeared on the CISA examination and references where additional guidance can be found. 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 *CISA Review Questions, Answers & Explanations Manual 2006* consists of 625 multiple-choice study questions. These items appeared in the 2005 edition of the *CISA Review Questions, Answers & Explanations Manual* and in the *2005 Supplement*, but many have been enhanced or rewritten to recognize a change in practice, be more representative of the current exam question format, and/or provide further clarity or explanation of the suggested correct answer. These questions are not actual test items, but are intended to provide the CISA candidate with an understanding of the type and structure of questions and subject matters that have previously appeared on the examination. Questions are sorted by CISA process and content areas and a sample test is provided. This publication is ideal for use in conjunction with the *CISA Review Manual 2006*.
- A *CISA Review Questions, Answers & Explanations Manual Supplement* is developed each year by ISACA. The 2006 edition consists of 100 new sample questions, answers and explanations for candidates to use in preparation for the CISA exam. The *2006 Supplement* was created based on the new CISA job practice, using a similar process for item development as that used to develop actual exam items. This publication is ideal to use in conjunction with the *CISA Review Manual 2006* and the *CISA Review Questions, Answers & Explanations Manual 2006*.
- CISA Review Questions, Answers & Explanations CD-ROM 2006 consists of the 725 questions, answers and explanations included in the *CISA Review Questions, Answers & Explanations Manual 2006* and the *CISA Review Questions, Answers & Explanations Manual 2006 Supplement*. All the questions are sorted based on the new 2006 CISA job practice. With this product, CISA candidates can identify strengths and weaknesses by taking various-length, random sample exams and reviewing the results by area. Sample exams also can be chosen by area, allowing for concentrated study, and by other sort features, such as the omission of previous correctly answered questions. Also included are *Information Systems Control Journal*® articles referenced in the *CISA Review Manual 2006*. The CD-ROM requires Windows 3.1 or above and a JavaScript 1.1-enabled browser, such as Netscape Communicator 4.05 or Internet Explorer 4.0 (ver 4.72) or above.
- CISA review courses are conducted by many ISACA chapters. Exam candidates should contact their local ISACA chapter to find out if a review course is being offered. These courses are often taught by current CISAs who present and discuss exam topics and share their secrets of success. Information pertaining to chapter contacts and course offerings is available at www.isaca.org/chapters and www.isaca.org/cisaexam, respectively. A two-day review course is also planned preceding the ISACA North America CACS conference 6-7 May 2006 in Orlando, Florida, USA.



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

Candidate's Guide to the CISA Exam

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 from the testing agency 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 your eTicket, you must have a current email address on file. If your email address changes, please update your Profile on our website or contact certification@isaca.org.

It is imperative that you note the specific registration and exam time on your 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 or her registration fee. You can use your admission ticket only at the designated test center specified on your admission ticket.

If you have not received your admission ticket by 1 June 2006 for the June administration or by 1 December 2006 for the December administration, please contact the CISA certification department immediately at certification@isaca.org or +1.847.253.1545, ext. 403, 471 or 474.

Be Prompt

Registration will begin at the time indicated on your 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.**

Remember to Bring Your 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 identification** will be admitted. Examples of acceptable forms of identification include those with a photo (e.g., a passport or photo driver's license). Any candidate who does not provide an original form of identification will not be allowed to sit for the exam and will forfeit his or 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.

Candidate's Guide to the CISA Exam

Be Careful in Completing the Answer Sheet

- An example of the multiple-choice answer sheet is included to familiarize candidates with its format. While many candidates have taken multiple-choice question exams, there are others who have never experienced a multiple-choice question exam.
- 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 writing 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 Your 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 Yourself Properly

- To protect the security of the exam and maintain the validity of the scores, candidates are asked to sign the answer sheet.
- The ISACA 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.

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 is scored using a method that utilizes a standard of performance established by a panel of content experts. A passing score (cut score) is set as the number of questions that a qualified candidate should answer correctly. Because variations exist from one exam to the next, the results of each exam after the cut score has been established are equated. Equating allows uniformity in the grading process and the resultant scaled scores reflect a comparable level of proficiency regardless of when the exam was taken. This scaled passing score represents neither a specific raw score nor a percentage of questions answered correctly.

At the conclusion of each exam, test questions are reviewed. Questions identified as being ambiguous or having technical or language flaws are either not used in the grading process or are given multiple correct answer keys. Raw scores are then arithmetically converted to scaled scores. A scaled score of 75 or above represents a passing score for the entire exam.

Candidate's Guide to the CISA Exam

Test scores are not available until approximately six (6) 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, fax or e-mail. Candidates can request an e-mail pass/fail status and score by marking the appropriate box on the CISA exam registration form.

Candidates will receive a score report containing a sub score for each job 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 Bulletin of Information. The sub scores can be useful in identifying those areas in which the candidate may need further study before retaking the exam. Unsuccessful candidates should note that taking either a simple or weighted average of the sub-scores 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. You 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 6 months after the exam was administered. If you apply after the deadline date, your request 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. Many times a CISA exam question will require the candidate to choose the appropriate answer that is **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 Questions, Answers & Explanations Manual*, and are examples of the CISA question format.

1. During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:
 - A. create the procedures document.
 - B. terminate the audit.
 - C. conduct compliance testing.
 - D. **identify and evaluate existing practices.**
2. In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?
 - A. Diskless workstations
 - B. Data encryption techniques
 - C. **Network monitoring devices**
 - D. Authentication systems
3. After completing the business impact analysis (BIA), which of the following is the next step in the business continuity process?
 - A. Test and maintain the plan.
 - B. Develop a specific plan.
 - C. **Develop recovery strategies.**
 - D. Implement the plan.

Candidate's Guide to the CISA Exam

4. In regard to moving an application program from the test environment to the production environment, the **BEST** control would be provided by having the:
- A. application programmer copy the source program and compiled object module to the production libraries.
 - B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
 - C. production control group compile the object module to the production libraries using the source program in the test environment.
 - D. production control group copy the source program to the production libraries and then compile the program.**
5. Which of the following represents the **GREATEST** potential risk in an EDI environment?
- A. Transaction authorization**
 - B. Loss or duplication of EDI transmissions
 - C. Transmission delay
 - D. Deletion or manipulation of transactions prior to or after establishment of application controls

Correct answers to the above questions are in bold. For explanations of correct and incorrect choices to these questions and for additional study questions, please refer to ISACA's *CISA Questions, Answers & Explanations Manual*.

CISA Exam Terminology

The CISA exam is offered in many languages. 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 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 information systems audit, control 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, operating or programming experience, or one year of financial or operational auditing experience can be substituted for one year of information systems auditing, control 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 information systems auditing, control or security experience.
- A bachelor's degree from a university that enforces the ISACA sponsored Model Curricula can be substituted for one year of information systems auditing, control or security experience. To view a list of these schools, please visit <http://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, information systems auditing) may be substituted for one year of information systems auditing, control 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.

Candidate's Guide to the CISA Exam

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

The CISA Continuing Education Policy requires the attainment of continuing education hours over an annual and three-year reporting period. CISAs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 continuing professional education hours.
- Submit annual continuing education maintenance fees to ISACA International Headquarters in full.
- Attain and report a minimum of 120 continuing professional education hours for a three-year reporting period.
- Respond and submit required documentation of continuing education 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 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

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

Content of the CISA Exam

The content of the exam is continuously modified to reflect changes in technology and practices. Every five years, 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 definitions.

Note: The percentages below indicate the emphasis or percent of questions that will appear on the exam from each area. The pages that follow contain further information regarding the specific tasks and knowledge statements that may be covered on the exam.

Content Areas

The IS Audit Process (10%)

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.

IT Governance (15%)

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.

Systems and Infrastructure Life Cycle Management (16%)

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.

IT Service Delivery and Support (14%)

Provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.

Protection of Information Assets (31%)

Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

Business Continuity and Disaster Recovery (14%)

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.

Candidate's Guide to the CISA Exam

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

Candidate's Guide to the CISA Exam

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 lifecycle 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 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 post-implementation 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 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

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 post-implementation 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

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

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

The CISA Examination and COBIT

COBIT, now in its fourth edition (COBIT 4.0), is an initiative conducted by the IT Governance Institute. COBIT has been developed as a generally applicable and accepted framework for good information technology 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 could 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 do reflect the tasks identified in the CISA practice analysis. 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. It includes a reference and cross-reference to both COBIT 3rd Edition as well as COBIT 4.0.

COBIT 3 rd Edition		COBIT4.0	
DOMAIN	PROCESS	DOMAIN	PROCESS
Plan and Organize		Plan and Organize	
PO1	Define a strategic IT plan.	PO1	Define a strategic IT plan.
PO2	Define the information architecture.	PO2	Define the information architecture.
PO3	Determine technological direction.	PO3	Determine technological direction.
PO4	Define the IT organization and relationships.	PO4	Define the IT processes, organisation and relationships.
PO5	Manage the IT investment.	PO5	Manage the IT investment.
PO6	Communicate management aims and direction.	PO6	Communicate management aims and direction.
PO7	Manage human resources.	PO7	Manage IT human resources.
PO8	Ensure compliance with external requirements.	PO8	Manage quality.
PO9	Assess risks.	PO9	Assess and manage IT risks.
PO10	Manage projects.	PO10	Manage projects.
PO11	Manage quality.		
Acquire and Implement		Acquire and Implement	
AI1	Identify automated solutions.	AI1	Identify automated solutions.
AI2	Acquire and maintain application software.	AI2	Acquire and maintain application software.
AI3	Acquire and maintain technology infrastructure.	AI3	Acquire and maintain technology infrastructure.
AI4	Develop and maintain procedures.	AI4	Enable operation and use.
AI5	Install and accredit systems.	AI5	Procure IT resources.
AI6	Manage changes.	AI6	Manage changes.
		AI7	Install and accredit solutions and changes.
Deliver and Support		Deliver and Support	
DS1	Define and manage service levels.	DS1	Define and manage service levels.
DS2	Manage third-party services.	DS2	Manage third-party services.
DS3	Manage performance and capacity.	DS3	Manage performance and capacity.
DS4	Ensure continuous service.	DS4	Ensure continuous service.
DS5	Ensure systems security.	DS5	Ensure systems security.
DS6	Identify and allocate costs.	DS6	Identify and allocate costs.
DS7	Educate and train users.	DS7	Educate and train users.
DS8	Assist and advise customers.	DS8	Manage service desk and incidents.
DS9	Manage the configuration.	DS9	Manage the configuration.
DS10	Manage problems and incidents.	DS10	Manage problems.
DS11	Manage data.	DS11	Manage data.
DS12	Manage facilities.	DS12	Manage the physical environment.
DS13	Manage operations.	DS13	Manage operations.
Monitor and Evaluate		Monitor and Evaluate	
M1	Monitor the process.	ME1	Monitor and evaluate IT performance.
M2	Assess internal control adequacy.	ME2	Monitor and evaluate internal control.
M3	Obtain independent assurance.	ME3	Ensure regulatory compliance.
M4	Provide for independent audit.	ME4	Provide IT governance.

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
The IS Audit Process		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.	PO9 Assess risk	PO9 Assess and manage IT risks
	M3 Obtain independent assurance	ME2 Monitor and evaluate internal control
	M4 Provide for independent audit	
Plan specific audits to ensure that IT and business systems are protected and controlled.	M3 Obtain independent assurance	ME2 Monitor and evaluate internal control
	M4 Provide for independent audit	
Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.	M4 Provide for independent audit	
Communicate emerging issues, potential risks and audit results to key stakeholders.	M3 Obtain independent assurance	PO9 Assess and manage IT risks
	M4 Provide for independent audit	ME2 Monitor and evaluate internal control
Advise on the implementation of risk management and control practices within the organization while maintaining independence.	PO9 Assess risk	PO9 Assess and manage IT risks
	PO11 Manage quality	PO8 Manage quality
	M3 Obtain independent assurance	
	M4 Provide for independent audit	
IT Governance		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Evaluate the effectiveness of 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.	PO1 Define a strategic IT plan	PO1 Define a strategic IT plan
	PO4 Define the IT organisation and relationship	PO4 Define the IT processes, organisation and relationships
	PO5 Manage the IT investment	PO5 Manage the IT investment
	PO6 Communicate management aims and directions	PO6 Communicate management aims and direction
	M2 Assess internal control adequacy	ME4 Provide IT governance
	M3 Obtain independent assurance	
	M4 Provide for independent audit	

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
IT Governance (continued)		
Tasks	COBIT 3rd Edition	COBIT 4.0
Evaluate IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.	PO4 Define the IT organisation and relationships	PO4 Define the IT processes, organisation and relationships
	PO7 Manage human resources	PO7 Manage IT human resources
	DS1 Define and manage service levels	DS1 Define and manage service levels
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.	PO1 Define a strategic IT plan	PO1 Define a strategic IT plan
	PO5 Manage the IT investment	PO5 Manage the IT investment
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.	PO8 Ensure compliance with external requirements	ME4 Provide IT governance
	AI6 Manage changes	AI6 Manage changes
	M1 Monitor the processes	ME1 Monitor and evaluate IT performance
Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standards and procedures.	PO6 Communicate management aims and direction	PO6 Communicate management aims and direction
	PO7 Manage human resources	PO7 Manage IT human resources
	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	DS6 Identify and allocate costs	DS6 Identify and allocate costs
Evaluate IT resource investment, use and allocation practices to ensure alignment with the organization's strategies and objectives.	PO5 Manage the IT investment	PO5 Manage the IT investment
	PO10 Manage projects	PO10 Manage projects
Evaluate IT contracting strategies and policies and contract management practices to ensure that they support the organization's strategies and objectives.	PO7 Manage human resources	PO7 Manage IT human resources
	PO8 Ensure compliance with external requirements	ME4 Provide IT governance
	AI1 Identify automated solutions	AI1 Identify automated solutions
	DS2 Manage third-party services	DS2 Manage third-party services
	DS9 Manage the configuration	DS9 Manage the configuration

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
IT Governance (continued)		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Evaluate risk management practices to ensure that the organization's IT-related risks are properly managed.	PO1 Define a strategic IT plan	PO1 Define a strategic IT plan
	PO6 Communicate management aims and directions	PO6 Communicate management aims and directions
	PO9 Assess Risk	PO9 Assess and manage IT risks
	PO10 Manage projects	PO10 Manage projects
	M1 Monitor the process	ME3 Ensure regulatory compliance
	M4 Provide for independent audit	
Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.	PO8 Ensure compliance with external requirements	ME4 Provide IT governance
	PO10 Manage Projects	PO10 Manage Projects
	PO11 Manage quality	PO8 Manage quality
	M2 Assess internal control adequacy	ME2 Monitor and evaluate internal control
	M3 Obtain independent assurance	
Systems and Infrastructure Lifecycle Management		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organization's business goals.	PO3 Determine technological direction	PO3 Determine technological direction
	PO11 Manage quality	PO8 Manage quality
	AI1 Identify automated solutions	AI1 Identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	DS9 Manage the configuration	DS9 Manage the configuration
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.	PO9 Assess risks	PO9 Assess and manage IT risks
	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	AI1 identify automated solutions	AI1 identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
Systems and Infrastructure Lifecycle Management (continued)		
Tasks	COBIT 3 rd Edition	COBIT 4.0
Perform reviews to ensure that a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.	PO10 Manage projects	PO10 Manage projects
	AI1 Identify automated solutions	AI1 Identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	M3 Obtain independent assurance	ME2 Monitor and evaluate internal control
	M4 Provide for independent audit	
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.	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	AI1 identify automated solutions	AI1 identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organization's objectives.	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	AI1 Identify automated solutions	AI1 Identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.	PO3 Determine technological direction	PO3 Determine technological direction
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
Perform post-implementation review of systems and/or infrastructure to ensure that they meet the organization's objectives and are subject to effective internal control.	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
Systems and Infrastructure Lifecycle Management (continued)		
Tasks	COBIT 3 rd Edition	COBIT 4.0
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.	PO6 Communicate management aims and direction	PO6 Communicate management aims and direction
	PO10 Manage projects	PO10 Manage projects
	PO11 Manage quality	PO8 Manage quality
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
	DS1 Define and manage service levels	DS1 Define and manage service levels
	DS3 Manage performance and capacity	DS3 Manage performance and capacity
	M2 Assess internal control adequacy	ME2 Monitor and evaluate internal control
	M3 Obtain independent assurance	
	M4 Provide for independent audit	
Evaluate the process by which systems and/or infrastructure are maintained to ensure the continued support of the organization's objectives and to ensure that they are subject to effective internal control.	PO3 Determine technological direction	PO3 Determine technological direction
	PO11 Manage quality	PO8 Manage quality
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	AI6 Manage Changes	AI6 Manage Changes
Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organization's policies and procedures.	PO6 Communicate management aims and direction	PO6 Communicate management aims and direction
	AI1 Identify automated solutions	
	AI1 Identify automated solutions	

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
IT Service Delivery and Support		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Evaluate service level management practices to ensure that the level of service from internal and external service providers is defined and managed.	AI4 Develop and maintain procedures	AI4 Enable operation and use
	DS1 Define and manage service levels	DS1 Define and manage service levels
	DS2 Manage third-party services	DS2 Manage third-party services
	DS6 Identify and allocate costs	DS6 Identify and allocate costs
	DS8 Assist and advise customers	DS8 Manage service desk and incidents
	M1 Monitor the process	DS10 Manage problems
		ME1 Monitor and evaluate IT performance
Evaluate operations management to ensure that IT support functions effectively meet business needs.	PO9 Assess risks	PO9 Assess and manage IT risks
	AI4 Develop and maintain procedures	AI4 Enable operation and use
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
	DS13 Manage operations	DS13 Manage operations
	M2 Assess internal control adequacy	ME1 Monitor and evaluate IT performance
Evaluate data administration practices to ensure the integrity and optimization of databases.	PO2 Define the information architecture	PO2 Define the information architecture
	PO4 Define the IT organization and relationships	PO4 Define the IT processes, organisation and relationships
	AI1 Identify automated solutions	AI1 Identify automated solutions
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
	DS5 Ensure systems security	DS5 Ensure systems security
	M1 Monitor the process	ME1 Monitor and evaluate IT performance

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
IT Service Delivery and Support (<i>continued</i>)		
<i>Tasks</i>	COBIT 3 rd Edition	COBIT 4.0
Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives.	AI1 Identify automated solutions	AI1 Identify automated solutions
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
	DS1 Define and manage service levels	DS1 Define and manage service levels
	DS3 Manage performance and capacity	DS3 Manage performance and capacity
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
Evaluate change, configuration and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented.	PO11 Manage quality	PO8 Manage quality
	AI2 Acquire and maintain application software	AI2 Acquire and maintain application software
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	AI5 Install and accredit systems	AI7 Install and accredit solutions and changes
	AI6 Manage changes	AI6 Manage changes
	DS9 Manage the configuration	DS9 Manage the configuration
Evaluate problem and incident management practices to ensure that incidents, problems and errors are recorded, analyzed and resolved in a timely manner.	DS8 Assist and advise customers	DS8 Manage service desk and incidents
	DS10 Manage problems and incidents	DS10 Manage problems and incidents
	DS11 Manage data	DS11 Manage data
	M2 Assess internal control adequacy	ME1 Monitor and evaluate IT performance
Evaluate the functionality of the IT infrastructure (e.g., network components, hardware and system software) to ensure that it supports the organization's objectives.	PO3 Determine technological direction	PO3 Determine technological direction
	PO11 Manage quality	PO8 Manage quality
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	AI6 Manage changes	AI6 Manage changes

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
Protection of Information Assets		
<i>Tasks</i>	COBIT 3rd Edition	COBIT 4.0
Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.	AI6 Manage changes	AI6 Manage changes
	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS5 Ensure systems security	DS5 Ensure systems security
	DS10 Manage problems and incidents	DS10 Manage problems
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS5 Ensure systems security	DS5 Ensure systems security
	DS11 Manage data	DS11 Manage data
	DS13 Manage operations	DS13 Manage operations
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.	PO9 Assess risks	PO9 Assess risks
	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS12 Manage facilities	DS12 Manage the physical environment
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
		ME4 Provide IT governance
Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.	PO4 define the IT organization and relationships	PO4 Define the IT processes, organisation and relationships
	DS5 Ensure systems security	DS5 Ensure systems security
	DS12 Manage facilities	DS12 Manage the physical environment
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
		ME4 Provide IT governance

Candidate's Guide to the CISA Exam

CISA Practice Analysis Tasks	COBIT Processes	
Requirements and Issues (continued)		
Tasks	COBIT 3rd Edition	COBIT 4.0
Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.	PO8 Ensure compliance with external requirements	ME4 Provide IT governance
	AI3 Acquire and maintain technology infrastructure	AI3 Acquire and maintain technology infrastructure
	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS5 Ensure systems security	DS5 Ensure systems security
	DS11 Manage data	DS11 Manage data
	M1 Monitor the process	ME1 Monitor and evaluate IT performance
Business Continuity and Disaster Recovery		
Tasks	COBIT 3rd Edition	COBIT 4.0
Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing.	PO2 Define the information architecture	PO2 Define the information architecture
	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS11 Manage data	DS11 Manage data
Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.	DS4 Ensure continuous service	DS4 Ensure continuous service
	DS11 Manage data	DS11 Manage data
	DS12 Manage facilities	DS12 Manage the physical environment
	DS13 Manage operations	DS13 Manage operations
		ME4 Provide IT governance
Evaluate the organization's business continuity plan to ensure its ability to continue essential business operations during the period of an IT disruption.	DS4 Ensure continuous service	DS4 Ensure continuous service

Candidate's Guide to the CISA Exam

Reference Materials

Ahuja, Jay; "Identity Management: A Business Strategy for Collaborative Commerce," *Information Systems Control Journal*, vol. 6, 2003, p. 49-53

Alga, Nadia; "Increasing Security Levels," *Information Systems Control Journal*, vol. 2, 2002, p. 35-41

Alles, Michael; Alexander Kogan; Miklos Vasarhelyi; "Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems," *Information Systems Control Journal*, vol. 1, 2003, p. 37-40

Andrew, Chris; "Patch Management: An Effective Line of Defense for UNIX and Linux," *Information Systems Control Journal*, vol. 6, 2003, p. 33-35

APM Group Limited (APMG); PRINCE2™, www.prince2.org.uk

Archer, Clark; Michael Stinson; *Object-oriented Software Measures*, Software Engineering Institute, CMU/SEI-95-TR-002, USA, April 1995

Ashbourn, Julian; *Biometrics: Advanced Identity Verification—The Complete Guide*, Springer-Verlag, UK, 2000

Ashbourn, Julian; "Biometric White Paper," 1999, www.avanti.1to1.org/whitepaper.html

Ashley, Mitchell; "A Guide to Wireless Network Security," *Information Systems Control Journal*, vol. 3, 2004, p. 43-46

Ashley, Mitchell; "A Network Is Threatened by Its Own Endpoints," *Information Systems Control Journal*, vol. 1, 2005, www.isaca.org/jonline

Ataya, Georges; "Risk-aware Decision Making for New IT Investments," *Information Systems Control Journal*, vol. 2, 2003, p. 12-14

Bachmann, Felix; Len Bass; Jeromy Carriere; Paul Clements; David Garlan; James Ivers; Robert Nord; Reed Little; *Software Architecture Documentation In Practice: Documenting Architectural Layers*, Software Engineering Institute, CMU/SEI-2000-SR-004, USA, March 2000

Bae, Benjamin B.; Paul Ashcroft; "Implementation of ERP Systems: Accounting and Auditing Implications," *Information Systems Control Journal*, vol. 5, 2004, p. 43-48

Bae, Benjamin; Ruth W. Epps; Susan S. Gwathmey; "Internal Control Issues: The Case of Changes to Information Processes," *Information Systems Control Journal*, vol. 4, 2003, p. 44-46

Bagranoff, Nancy A.; Laurie Henry; "Choosing and Using Sarbanes-Oxley Software," *Information Systems Control Journal*, vol. 2, 2005, p. 49-51

Bakalov, Rudy and Feisal Nanji; "Offshore Application Development Done Right," *Information Systems Control Journal*, vol. 5, 2005, p. 52-56

Bakalov, Rudy; "Risk Management Strategies for Offshore Application and Systems Development," *Information Systems Control Journal*, vol. 5, 2004, p. 36-38

Bakshi, Sunil; "Control Self-assessment for Information and Related Technology," *Information Systems Control Journal*, vol. 1, 2004, p. 55-62

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Bank for International Settlements, *Basle Committee on Banking Supervision—Risk Management Principles for Electronic Banking*, Switzerland, May 2001

Barbin, Douglas; John Patzakis; “Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program,” *Information Systems Control Journal*, vol. 3, 2002, p. 25-27

Barrett, Neil; *Traces of Guilt*; Transworld Publishing, UK, 2004

Basel Committee on Banking Supervision, “Risk Management Principles for Electronic Banking,” Basle Directive N° 82, Switzerland, May 2001

Basel Committee on Banking Supervision, “Sound Practices for the Management and Supervision of Operational Risk,” Basle Directive N° 86, Switzerland, May 2001

Basel Committee on Banking Supervision, “Risk Management Principles for Electronic Banking,” Basle Directive N° 91, Switzerland, July 2002

Bayuk, Jennifer L.; *Stepping Through the IS Audit: What to Expect. How to Prepare, 2nd Edition*, Information Systems Audit and Control Association, USA, 2004

Bek, Jon; “ZFP Audit: A Computer-assisted Audit Tool for Evaluation of Microsoft Operating Systems,” *Information Systems Control Journal*, vol. 1, 2004, p. 34-37

Benvenuto, Nick; David Brand; “Managing the Risk of Outsourcing in a Post-Sarbanes World,” *Information Systems Control Journal*, vol. 5, 2004, p. 31-33

Benvenuto, Nicholas A.; David Brand; “Outsourcing—A Risk Management Perspective,” *Information Systems Control Journal*, vol. 5, 2005, p. 35-40

Bhatia, Mohan; “New Basel Accord: Operational Risk Management—Emerging Frontiers for the Profession,” *Information Systems Control Journal*, vol. 1, 2002, p. 37-42

Bhatia, Mohan; “Web Services Security,” *Information Systems Control Journal*, vol. 1, 2005, p. 45-48

Bindseil, James; “Wise Wireless: Securing the WLAN,” *Information Systems Control Journal*, vol. 6, 2003, p. 25-26

Bindseil, James; “Wise Wireless: Securing the WLAN,” *Information Systems Control Journal*, vol. 6, 2003, p. 25-26

Bitterli, Peter R; “IT Security Governance—A Slow Start to a High Maturity Level,” *Information Systems Control Journal*, vol. 1, 2005, p. 16-19

Blanco, Luis; “Audit Trails in an E-commerce Environment,” *Information Systems Control Journal*, vol. 5, 2002, p. 32-35

Bozdoc, Marian; “CAD Chronology,” Resources and Information for Professional Designers web site, New Zealand, 2003, <http://mbinfo.mbdesign.net/CAD1970.htm>

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

Bradley, K.; *Ken Bradley's Understanding PRINCE2*, SPOCE Project Management Limited, UK, 1999

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Bragg, Tom; "Designing and Building Software Projects: Lessons From the Building Trades," *Agile Project Management Advisory Service*, vol. 3, No. 10, 2002, www.cutter.com/project/abstracts.html

Brancik, Kenneth C.; "The Computer Forensics and Cybersecurity Governance Model," *Information Systems Control Journal*, vol. 2, 2003, p. 41-47

Brasche, Randy "Eliminating Today's Costly Outsourcing Operations Challenges," *Information Systems Control Journal*, vol. 5, 2004, p. 34-35

Braswell, Daniel E.; W. Ken Harmon; "Assessing and Preventing Risks from E-mail System Use," *Information Systems Control Journal*, vol. 5, 2003, p. 33-35

Briner, M.; M. Geddes; C. Hastings; *Project Leadership, 2nd Edition*, Gower, UK, 2001

British Standard Institute; "Information Technology—Code of Practice for Information Security Management," BS ISO/IEC 17799:2000

Bromba, Manfred; "Biometrics," Bioidentification, <http://home.t-online.de/home/manfred.bromba/biofaq.htm>

Bunker, Eva; "Optimizing an Organization's Security Effectiveness by Using Vulnerability Management to Support the Audit Function," *Information Systems Control Journal*, vol. 4, 2003, p. 28-30

Business Continuity Institute, "Business Continuity Management Standards," UK, 2003, www.thebci.org/certification_standards.html

Business Continuity Institute, "Good Practice Guidelines," UK, 2002, www.thebci.org/BCI%20GPG%20-%20Introduction.pdf

Business Continuity Institute, "Good Practices for Business Continuity Management," UK, 2004, www.thebci.org/GPGMain.html

Butler, Charles W.; Gary L. Richardson; "Potential Control Processes for Sarbanes-Oxley Compliance," *Information Systems Control Journal*, vol. 2, 2005, www.isaca.org/jonline

Byrne, Jim; "Large-scale Biometric Management: Centralized, Policy-based Approach to Reducing Organizational Identity Chaos," *Information Systems Control Journal*, vol. 6, 2003, p. 41-44

Caldwell, Matthew; "The Importance of Event Correlation for Effective Security Management," *Information Systems Control Journal*, vol. 6, 2002, p. 37-38

Carasik, Anne; "Choosing the Best Solution for Your Network Security: Secure Shell, TLS or IPSec," *Information Systems Control Journal*, vol. 3, 2001, p. 33-39

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

Caupin, G.; H. Knöpfel; Peter W. G. Morris; Erhard Motzel; Olaf Pannenbäcker; *ICB—IPMA Competence Baseline*, IPMA Bremen, Germany, 1999

Central Computer and Telecommunications Agency, *Managing Successful Programmes*, UK, 1999

Cerullo, Michael J.; Virginia Cerullo; "Threat Assessment and Security Measures Justification for Advanced IT Networks," *Information Systems Control Journal*, vol. 1, 2005, p. 35-43

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

Cerullo, Virginia M; Michael J. Cerullo; "Impact of SAS No. 94 on Computer Audit Techniques," *Information Systems Control Journal*, vol. 1, 2003, p. 53-57

Champlain, Jack J.; *Auditing Information Systems, 2nd Edition*, John Wiley & Sons, USA, 2003

Champlain, Jack; *Practical IT Auditing, 2nd Edition*, Warren Gorham & Lamont, USA, 2002

Chan, David; "What Auditors Should Know About Encryption," *Information Systems Control Journal*, vol. 3, 2004, p. 30-34

Chapin, David A.; Steven Akridge; "How Can Security Be Measured?," *Information Systems Control Journal*, vol. 2, 2005, p. 43-47

Chapman, C.; R. Turner (Ed.); "Risk Management," *The Commercial Project Manager*, McGraw Hill, UK, 1995

Chapman, C.; Stephen Ward; *Project Risk Management—Processes, Techniques and Insights*, John Wiley & Sons, USA, 1997

Chappell, David; *Taking Stock of Component Technology*, Chappell & Associates, USA, June 1999

Chappell, David; *The Next Wave: Component Software Enters the Mainstream*, Chappell & Associates, USA, April 1997

Chavan, Umesh; "An Approach to Vulnerability Management," *Information Systems Control Journal*, vol. 5, 2005, www.isaca.org/jonline

Cheung, Humphrey; "The Feds Can Own Your WLAN Too," TomsNetworking, 2005, www.tomsnetworking.com/Sections-article111-page1.php

Cilli, Claudio; "IT Governance: Why a Guideline?," *Information Systems Control Journal*, vol. 3, 2003, p. 22-24

Cleland, D.I.; *Project Management—Strategic Design and Implementation*, McGraw Hill, USA, 2002

Cleland, D.I.; R. Gareis (Ed.); *Global Project Management Handbook*, McGraw Hill, USA, 1994

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

Cohen, Gidi; "The Role of Attack Simulation in Automating Security Risk Management," *Information Systems Control Journal*, vol. 1, 2005, p. 51-54

Comptroller of the Currency Administration of National Banks, *Large Bank Supervision—Comptroller's Handbook*, USA, May 2001

Cronin, Mary J.; *Banking and Finance on the Internet*, John Wiley & Sons, USA, 1997

Cutter Information Corp., *An Overview of E-business Architecture*, Component Development Strategies, USA, April 2001

Danielyan, Edgar; "IEEE802.11," *The Internet Protocol Journal*, vol. 5, no. 1, March 2002, Cisco, www.cisco.com/warp/public/759/ipj_5-1.pdf

Dartmouth AI Conference, "Internet History," http://livinginternet.com/i/ii_ai.htm

Debenham, John; *Knowledge Engineering: Unifying Knowledge Base and Database Design*, Springer Verlag, 2001

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

De Haes, Steven; Wim Van Grembergen; "IT Governance and its Mechanisms," *Information Systems Control Journal*, vol. 1, 2004, p. 27-33

Deitel, Harvey M.; *Introduction to Operating Systems, 2nd Edition*, Addison-Wesley, 1990

Denker, Bob; "Analysis Software for Auditors and Management," *Information Systems Control Journal*, vol. 1, 2001, p. 25-26

Denning, Dr. Dorothy L.; *Information Warfare*, ACM Press Books, USA, 1999

Dimitriadis, Christos K.; Despina Polemi; "Biometrics—Risks and Controls," *Information Systems Control Journal*, vol. 4, 2004, p. 41-43

Disaster Recovery Institute International, "Professional Practices for Business Continuity Professionals," 2004, www.drii.org/displaycommon.cfm?an=2

Doughty, Ken; "Implementing Enterprise Security: A Case Study (Part1)," *Information Systems Control Journal*, vol. 2, 2003, p. 34-39

Doughty, Ken; "Implementing Enterprise Security: A Case Study (Part2)," *Information Systems Control Journal*, vol. 3, 2003, p. 60-63

Doughty, Ken; Frank Grieco; "IT Governance: Pass or Fail?," *Information Systems Control Journal*, vol. 2, 2005, www.isaca.org/jonline

Doughty, Ken; John O'Driscoll; "Information Technology Auditing and Facilitated Control Self-assurance," *Information Systems Control Journal*, vol. 4, 2002, p. 33-38

Down, Michael P.; Richard J. Sands; "Biometrics: An Overview of the Technology, Challenges and Control Considerations," *Information Systems Control Journal*, vol. 4, 2004, pages 53-56

Driml, Scott; "Enhancing Security With an IT Network Awareness Center," *Information Systems Control Journal*, vol. 4, 2003, p. 51-52

Echenique García, José Antonio; *Auditoría en Informática, 2a. Edición*, McGraw Hill, Mexico, 2002

Edwards Information LLC; *Disaster Recovery Yellow Pages, 14th Edition*, USA, 2005

ERP Knowledgebase; *Information Technology Tool Box*, USA, 2004, <http://erp.ittoolbox.com>

Essinger, James; *The Virtual Banking Revolution*, Thomson Business Press, UK, 1998

Farris, Greg; "Effective Encryption Requires an Integrated System," *Information Systems Control Journal*, vol. 4, 2004, p. 46-47

Federal Emergency Management Agency, "Emergency Management Guide for Business & Industry," USA, 2000, www.FEMA.gov/library/prepandprev.shtm/bisindst.pdf

Federal Emergency Management Agency, "Mitigation An Investment for the Future," USA, 1999, www.FEMA.gov/library/prepandprev.shtm/mit_baldwin.doc

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Federal Reserve Bank of Chicago, *An Internet Banking Primer*, USA, 2005

Ford, Merilee; H. Kim Lew; Steve Spanier; Tim Stevenson; *Internetworking Technologies Handbook, 3rd Edition*, Cisco Press, USA, 2000

Ford, Stephen; "Security in the Land Down Under," *Information Systems Control Journal*, vol. 6, 2003, p. 62-64

Frelinger, Bob; "Building Acceptance and Adoption of COBIT at Sun Microsystems," *Information Systems Control Journal*, vol. 2, 2005, p. 23-28

Frownfelter-Lohrke, Cynthia; James E. Hunton; "New Opportunities for Information System Auditors: Linking SysTrust to COBIT," *Information Systems Control Journal*, vol. 3, 2002, p. 45-48

Gallegos, Frederick; "Due Professional Care," *Information Systems Control Journal*, vol. 2, 2002, p. 25-28

Gallegos, Frederick; "Educating the Masses: Audit, Control and Security of Information Systems Today and Tomorrow," *Information Systems Control Journal*, vol. 6, 2004, p. 13-15

Gallegos, Frederick; "Maintaining IT Audit Proficiency—The Role of Professional Development Planning," *Information Systems Control Journal*, vol. 6, 2002, p. 20-23

Gallegos, Frederick; "Sarbanes-Oxley Status," *Information Systems Control Journal*, vol. 2, 2005, p. 11-13

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

Garfinkel, Simson; Gene Spafford; *Web Security, Privacy and Commerce, 2nd Edition*, O'Reilly & Associates, USA, 2002

Garside, T.; C. Pedersen; "Basel II Prompts Strategic Rethinks," *Euromoney*, December 2002

Gaulke, Markus; "Risk Management in IT Projects," *Information Systems Control Journal*, vol. 5, 2002, p. 37-39

Gerdes, Michael; "An Exploration of Global Perceptions of Security and Privacy," *Information Systems Control Journal*, vol. 6, 2002, p. 27-30

Giarratano, Joseph C.; *Expert Systems: Principles and Programming, 3rd Edition*, PWS Publishing Company, 1998

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

Gold, Robert S.; "Enabling the Strategy-focused IT Organization," *Information Systems Control Journal*, vol. 4, 2002, p. 21-23

Gorgoglione, Janice; Gilbert W. Joseph; "Laser Check Printing—How It Effects the Internal Control System," *Information Systems Control Journal*, vol. 4, 2002, p. 39-47

Gower, Aldershot; Turner, J.R.; St.J. Simister; (Eds.), *Gower Handbook of Project Management*, UK, 2000

Greene, Fredric; "A Survey of Application Security in Current International Standards," *Information Systems Control Journal*, vol. 6, 2002, p. 47-51

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Griss, Martin L.; Ivar Jacobson; "Component-based Development: Approaching the Promised Land of Component Reuse," ADTmag.com, June 2001

Guldentops, Erik; "IT Dimension of Basel II," *Information Systems Control Journal*, vol. 6, 2004, p. 17-19

Gupta, Ajay; Scott Laliberte; *Defend IT*, Addison Wesley, USA, 2004

Hale, Ron; "Helping Businesses Safeguard Information and Networks," *Information Systems Control Journal*, vol. 1, 2001, p. 23

Hamaker, Stacey; "Spotlight on Governance," *Information Systems Control Journal*, vol. 1, 2003, p. 15-19

Hamaker, Stacey; Austin Hutton; "Principles of Governance," *Information Systems Control Journal*, vol. 3, 2003, p. 44-49

Hamaker, Stacey; Austin Hutton; "Principles of IT Governance," *Information Systems Control Journal*, vol. 2, 2004, p. 47-50

Hammer, M.; *The Agenda: What Every Business Must Do to Dominate the Decade*, Crown Business, USA, 2001

Hardy, Gary; "Make Sure Management and IT Are on the Same Page: Implementing an IT Governance Framework," *Information Systems Control Journal*, vol. 3, 2002, p. 14-16

Harmon, Roy L.; *Reinventing the Factory II*, Free Press, USA, 1991

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

Harrison, Robert M.; "Application Risk in a TCP/IP Environment," *Information Systems Control Journal*, vol. 2, 2002, vol. 6, 2002, p. 39-40

Hawker, Andrew; "Security and Controls in Information Security," *Routledge Information Systems Textbook*, 2000, p. 151

Hernández Hdez, Enrique; *Auditoría de Informática: Un Enfoque Metodológico y Práctico*, Grupo Adneti, Mexico, 2004

Hernández Hdez., Enrique; *Administración y Seguridad de la Tecnología de Información: Metodología, Procesos y tareas claves*, Grupo Adneti, Mexico, 2005

Heschl, Jimmy; "COBIT in Relation to Other International Standards," *Information Systems Control Journal*, vol. 4, 2004, p. 37-40

Highsmith, Jim; Nancy R. Mead; Daniel J. Mosley; Balasubramaniam Ramesh; Lou Russell; Karl E. Wieggers; *Requirements Engineering and Management*, Cutter Information Corp., USA, July 2000

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

Hoskinson, Clayton; "Data Hiding," *Information Systems Control Journal*, vol. 3, 2002, p. 28-32

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Hug-Heuveneers, Christophe; "Enterprise Instant Messaging: Taking Control," *Information Systems Control Journal*, vol. 1, 2005

Huijgens, Hennie; "Value Chain Control—An IT Control Approach That Puts Business in the Centre," *Information Systems Control Journal*, vol. 2, 2004, p. 57-62

Humphries, John E.; "Preventing EFT Fraud," *Information Systems Control Journal*, vol. 4, 2003

Information Assurance Directorate; "U.S. Government Biometric Verification Mode Protection Profile (PP) for Medium Robustness Environments," 15 November 2003, www.commoncriteriaportal.org/public/files/ppfiles/pp_vid1022-pp.pdf

Information Headquarters, "IEEE 802.11 (Wi-Fi)," 2004, www.informationheadquarters.com/Apple_Macintosh/IEEE_80211b.shtml

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

Information Systems Audit and Control Association, *CISM Review Manual 2005*, USA, 2005, p.137

Information Systems Audit and Control Association, IS Auditing Procedure No. 1, IS Risk Assessment Measurement, USA, 2002

Information Systems Audit and Control Association, IS Auditing Standard S6 Performance of Audit Work, 04 Evidence, USA, 2005

Information Systems Audit and Control Association, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, USA, 2005, www.isaca.org/standards.

Information Systems Audit and Control Association; *Cybercrime: Incident Response & Digital Forensics*, USA, 2005

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

International Organization for Standardization and International Electrotechnical Commission (IEC); *Information Technology—Guidelines for the Management of IT Security* (TR 13335-1), Subcommittee 27, Working Group 1, 1996

International Organization for Standardization, "Quality Management Principles," ISO 9000, UK, 2000

International Organization for Standardization, "Quality Management Systems—Requirements," ISO 9001, UK, 2000

International Organization for Standardization, "Quality Management Systems—Guidelines for Performance Improvements," ISO 9004, UK, 2000

International Organization for Standardization, "Software Engineering—Product Qualify," ISO 9126, UK, 2001, 2003, 2004

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

International Project Management Association (IPMA), www.ipma.ch

The Internet Engineering Taskforce, "Telnet TN3270 Enhancements," www.ietf.org/proceedings/97aug/transit97aug-28.htm

The Internet Engineering Taskforce, "Transport Layer Security (TLS)," www.ietf.org/html.charters/tls-charter.html

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

The Internet Society, RFC 2828—Internet Security Glossary, May 2000, www.faqs.org/rfcs/rfc2828.html

The Internet Society, RFC 2401—Security Architecture for the Internet Protocol, November 1998, www.faqs.org/rfcs/rfc2401.html

IPL Information Processing Limited, "Software Testing and Software Development Life Cycles," UK, 1996

Information Systems Audit and Control Association Standards Board; "Effect of Third Parties on an Organization's IT Controls," *Information Systems Control Journal*, vol. 4, 2002, p. 28-31

Information Systems Audit and Control Association; IS Auditing Guideline, G28 Computer Forensics, USA, 2004

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

IT Governance Institute and Deloitte & Touche, *e-Commerce Security—Business Continuity Planning*, USA, 2002

IT Governance Institute and Deloitte & Touche, *e-Commerce Security—Enterprise Best Practices*, USA, 2000

IT Governance Institute and Deloitte & Touche, *e-Commerce Security—A Global Status Report*, USA, 2000

IT Governance Institute and Deloitte & Touche, *e-Commerce Security—Securing the Network Perimeter*, USA, 2002

IT Governance Institute and PricewaterhouseCoopers; *Risks of Customer Relationship Management*, USA, 2003

IT Governance Institute, COBIT 3rd Edition *Control Objectives*, 2000

IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, USA, 2004, www.isaca.org/sox

IT Governance Institute; *Security, Audit and Control Features SAP® R/3®—A Technical and Risk Management*, USA, 2002

Jamieson, Rodger; Greg Stephens; Santhosh Kumar; "Fingerprint Identification: An Aid to the Authentication Process," *Information Systems Control Journal*, vol. 1, 2005, www.isaca.org/jonline

Johner, Heinz; Seiei Fujiwara; Amelia Sm Yeung; Anthony Stephanou; Jim Whitmore; *Deploying a Public Key Infrastructure*, IBM, March 2000, p. 29-34, 49-52

Johnson, Everett C.; "IT Governance: New Players, Challenges and Opportunities," *Information Systems Control Journal*, vol. 2, 2005, p. 17-18

Johnson, Philip Avery; *Introduction to Operating Systems*, Hampton University, USA, 2004

Jones, Wayne; Leonidas Anzola; John Ho Chi; "Global Perspectives: IT Governance Regulation," *Information Systems Control Journal*, vol. 2, 2005, p. 20-22

Kan, A. H. G. Rinnooy; "IT Governance and Corporate Governance at ING," *Information Systems Control Journal*, vol. 2, 2004, p. 26-31

Keating, Stephen; Richard M. Smith; "Top US Privacy Stories of 2000," *Information Systems Control Journal*, vol. 3, 2001, p. 29-31

Kennedy, Susan; "Best Practices for Wireless Network Security," *Information Systems Control Journal*, vol. 3, 2004, p. 36-38

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Kenny, Steve; "Assuring Data Privacy Compliance," *Information Systems Control Journal*, vol. 4, 2004, p. 31-33

Kerzner, H.; *Project Management—A Systems Approach to Planning, Scheduling and Controlling, 7th Edition*, John Wiley & Sons, USA, 2001

Khan, Kamal; Rajan Syal; Achal Kapila; "Introduction to Voice-over IP Technology," *Information Systems Control Journal*, vol. 2, 2005, p. 54-56

Koblitz, Neal I.; *A Course in Number Theory and Cryptography*, Springer Verlag, USA, 1994

Koorn, Ronald; Peter van Walsem; Mark Lundin; "Auditing and Certification of a Public Key Infrastructure," *Information Systems Control Journal*, vol. 5, 2002, p. 28-31

Kordel, Luc; "IT Governance Hands-on: Using COBIT to Implement IT Governance," *Information Systems Control Journal*, vol. 2, 2004, p. 39-46

Krist, Martin A.; *Standard for Auditing Computer Applications*, Auerbach, USA, 1999

Lainhart, John W.; "Businesses Today Are Undergoing a Chemical Change," *Information Systems Control Journal*, vol. 1, 2001, p. 18-19

Lanza, Richard B.; "How to Use a New Computer Audit Fraud Prevention and Detection Tool," *Information Systems Control Journal*, vol. 1, 2004, p. 63-66

Ledesma, Cristina; John G. Ott; "Virtual Private Network (VPN): Audit Approach Based on Standards SDLC Concepts," *Information Systems Control Journal*, vol. 4, 2004, p. 23-24

Lee, Elsa; "Combating Cyberthreats—Partnership Between Public and Private Entities," *Information Systems Control Journal*, vol. 3, 2002, p. 38-43

Lubbe, Sam; "Documentation Standards for E-commerce Organisations," *Information Systems Control Journal*, vol. 5, 2003, p. 24-25

Lux, Allen G; Sandra Fitiani; "Fighting Internal Crime Before It Happens," *Information Systems Control Journal*, vol. 3, 2002, p. 50-51

Maconachy, William V.; Corey Schou; James Frost; John Springer; "Building an Educational Response to Terrorism: A Multifaceted Problem, A Multidimensional Response," *Information Systems Control Journal*, vol. 6, 2004, p. 42-47

Mahadevan, Chidambaram; "Intrusion, Attack, Penetration—Some Issues," *Information Systems Control Journal*, vol. 6, 2001, p.52-57

Maher, Mark; "Writing a Computer Forensic Technical Report," SANS Institute, 2004

Mandia, K.; C. Prorise; M. Pepe; *Incident Response, 2nd Edition*, McGraw-Hill/Osborne, 2003

ManTech Advanced Systems International Inc., *Security Architecture for an Internet-based Network*, 1998,
www.dcnicn.com/lamp/cals_97f/task04/doc/Security/security95.doc

Mantel, S.J.; J.R. Meredith; *Project Management—A Managerial Approach, 4th Edition*, John Wiley & Sons, USA, 2000

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

Mark, Robert; "Finding a Best-practices Method for Measuring Operational Risk," *Worldfinance*, vol. 12, Issue 2

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

McConnell, Steve; *Software Project Survival Guide*, Microsoft Press, USA, 1998

McCormack, K; "Business Process Orientation—What Is It and How Do You Know When You Have It?," USA, 1999, www.reengineering.com/press/survey1/BPOtopics.doc

McKinney, Charles; "Capability Maturity Models and Outsourcing: A Case for Sourcing Risk Management," *Information Systems Control Journal*, vol. 5, 2005, p. 28-34

McNamee, David; *Business Risk Assessment*, The Institute of Internal Auditors, USA, 1998, www.theiia.org

McQuaide, Bill; "Identity and Access Management," *Information Systems Control Journal*, vol. 4, 2003 p. 35-37

Menezes, Alfred; "Elliptic Curve Public Key Cryptosystems," Kluwer Academic, The Kluwer International Series in Engineering and Computer Science, Sec 234, Communications and Information, USA, 1993

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

Milus, Stu; "The Institutional Need for Comprehensive Auditing Strategies," *Information Systems Control Journal*, vol. 6, 2004, p. 51-56

Mitnick, Kevin; *The Art of Deception*, Wiley Publishing, USA, 2002

Mohay, George; Alison Anderson; Byron Collie; Olivier de Vel; D. Rodney McKemmish; *Computer and Intrusion Forensics*, UK, 2004

Monetary and Economic Department, Bank for International Settlements, BIS Papers N° 7., "Electronic Finance: A New Perspective and Challenges," Switzerland, November 2001

Moody, Robert; "Ports and Port Scanning: An Introduction," *Information Systems Control Journal*, vol. 5, 2001, p. 34-39

Mookhey, K.K.; "Common Criteria: An Overview," *Information Systems Control Journal*, vol. 1, 2005, p. 30-34

Mookhey, K.K.; "Open Source Tools for Security and Control Assessment," *Information Systems Control Journal*, vol. 1, 2004, p. 39-44

Murhammer, Martin W.; Orcun Atakan ;Stefan Bretz; Larry R. Pugh; Kazunari Susuki; David H. Wood; *TCP/IP Tutorial and Technical Overview*, IBM, 1998, p. 297 and 339

Musaji, Yusuf; "Conflict Resolution," *Information Systems Control Journal*, vol. 5, 2002, p. 47-50

Musaji, Yusuf; "Sarbanes-Oxley and Business Process Outsourcing Risk," *Information Systems Control Journal*, vol. 5, 2005, p. 47-49

Muthukrishnan, Ravi; "The Auditor's Prerogative to Review Internal Controls," *Information Systems Control Journal*, vol. 2, 2004, p. 54-56

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

Nachenberg, Carey; "Generic Exploit Blocking: Prevention, Not Cure," *Information Systems Control Journal*, vol. 2, 2005, www.isaca.org/jonline

Nagaraj, N.S.; "Business Process Management—An Emerging Trend," Infosys/SETLabs, India, 2001, www.fujitsu.com/downloads/SG/fapl/workflow/iflow_bpm.pdf

Nash, Andrew; William Duane; Celia Joseph; Derek Brink; PKI: Implementing and Managing E-security, RSA Press, USA, 2001

National Emergency Management Association, "National Incident Management System," USA, 2004, <http://nemaweb.org/docs/NIMS%20-%20Final%20Draft.pdf>

National Institute of Justice; "Electronic Crime Scene Investigation: A Guide for First Responders," USA, p. 98, www.ncjrs.org/pdffiles1/nij/187736.pdf

National Institute of Standards and Technology (NIST), "Security Considerations for Voice Over IP Systems," USA, 2005, www.nist.gov

National Institute of Standards and Technology (NIST), "Integration Definition for Information Modeling," USA, 2005, www.nist.gov

Nelson, William F.; Wei Lu; "Securing the Wireless Network," *Information Systems Control Journal*, vol. 3, 2004, p. 27-29

Niblett, Peter; Sander S. Wechsler; "The IS Auditor's Consideration of Irregularities and Illegal Acts," *Information Systems Control Journal*, vol. 3, 2003, p. 56-59

Nichols, Randall K.; Daniel J. Ryan; *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*, McGraw Hill, USA, 2000

Njemanze, Hugh S.; "Centralized Security Management Provides Foundation for Effective Intrusion Prevention," *Information Systems Control Journal*, vol. 4, 2003, p. 47-48

Norifusa, Masaya; "Securing Emerging Internet Applications," *Information Systems Control Journal*, vol. 2, 2001, p. 36-39

Norris, Robert C.; "Virtual Private Networking: Confidentiality on Public Networks," *Information Systems Control Journal*, vol. 3, 2001, p. 23-26

Office of Government Commerce (OGC); *Application Management*, The Stationary Office, UK, 2002

Office of Internal Audit Best Practices, "Internal Controls," Wayne State University, USA, 2005, <http://internalaudit.wayne.edu/Internal/Auditing%20Best%20Practices.doc>

Paliotta, Allan R.; "Cybersecurity and the Future of E-commerce: The Role of the Audit Community," *Information Systems Control Journal*, vol. 2, 2001, p. 29-30

Pareek, Mukul; "IT Governance and Post-merger Systems Integration," *Information Systems Control Journal*, vol. 2, 2005, p. 30-33

Parker, Xenia Ley, *Miller Information Technology Audits*, 2005 Edition, CCH Inc., 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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

- Parkes, Hugh; "IT Governance and Outsourcing," *Information Systems Control Journal*, vol. 5, 2004, p. 17-21
- Parkinson, Michael; "CPO Position Joins Executive Ranks," *Information Systems Control Journal*, vol. 3, 2001, p. 53-55
- Pathak, Jagdish; "Information Technology Auditing and Cybercommerce: A Risk Perspective," *Information Systems Control Journal*, vol. 6, 2004, p. 21-25
- Patzakis, John M.; "Computer Forensics—From Cottage Industry to Standard Practice," *Information Systems Control Journal*, vol. 2, 2001, p. 25-27
- Paulk, Marc C.; Charles V. Weber; Bill Curtis; Mary Beth Chrissis; *The Capability Maturity Model for Software: Guidelines for Improving the Software Process (SEI)*, Addison Wesley, 1995
- Pauls, Nicole; "Security Information Management: Not Just the Next Big Thing," *Information Systems Control Journal*, vol. 5, 2005, www.isaca.org/jonline
- Petroff, John N.; *Handbook of MRP II/JIT Integration and Implementation*, Prentice Hall, USA, 1993
- Pidanick, Ryan; "An Investigation of Computer Forensics," *Information Systems Control Journal*, vol. 3, 2004, p. 47-51
- Pikover, Yuri; Jeff Drake; *Security Provisioning: Managing Access in Extended Enterprises*, IT Governance Institute, USA, 2002
- Pinkett, Fred; "Automating System Security Audits," *Information Systems Control Journal*, vol. 1, 2004, p. 45-46
- Piper, Fred; "An Introduction to Cryptography," *Information Systems Control Journal*, vol. 6, 2003, p. 54-61
- Piper, Fred; Simon Blake-Wilson; John Mitchell; *Digital Signatures—Security and Controls*, IT Governance Institute, USA, 1999
- Pironti, John P; "Key Elements of an Information Security Program," *Information Systems Control Journal*, vol. 1, 2005, p. 23-28
- PricewaterhouseCoopers, "Strengthening Internal Audit's Role in Corporate Governance," March 2004, www.pwc.com/extweb/pwcpublishings.nsf/docid/2D6AFC4B68DE214A85256E830014E2C0
- Project Management Austria, *PM baseline*, Austria, 2002
- Project Management Forum (PMFORUM), www.pmforum.org
- Project Management Institute (PMI), www.pmi.org
- Project Management Institute, *A Guide to the Project Management Body of Knowledge*, USA, 2000
- Public Company Accounting Oversight Board, "An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements," Auditing Standard No. 2, USA, 2004
- Purdue University, "Computer Integrated Manufacturing Technology," USA, 2004, www.tech.purdue.edu/cimt/

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

Rafeq, A.; "Using COBIT for IT Control Health Check-up," *Information Systems Control Journal*, vol. 5, 2005, p. 18-19

Ramos, Daniel; "The Auditor's Role in IT Governance," *Information Systems Control Journal*, vol. 5, 2001, p. 23-24

Robb, Drew; "Protecting Ports—Using an Event Log Manager to Improve Network Security," *Information Systems Control Journal*, vol. 4, 2004, p. 44-45

Roberts, Barney B.; "The Benefits of Integrated, Quantitative Risk Management," Australia, 2001, www.futron.com/pdf/benefits_QuantIRM.pdf

Rollins, Steven; Richard Lanza; *Essential Project Investment Governance and Reporting Preventing Project Fraud and Ensuring Sarbanes-Oxley Compliance*, J. Ross Publishing, USA, 2005

Rosenthal, Paul H.; "Exercising Your Contingency Teams," Contingency Planning & Management web site; 2003, www.contingencyplanning.com/Tools/BCPHandbook/BCP201.asp

Ross, Steven J.; "Give 'em the New Razzle-Dazzle," *Information Systems Control Journal*, vol. 5, 2005, p. 9-10

Ross, Steven J.; "Information Security and the Resilient Enterprise," *Information Systems Control Journal*, vol. 2, 2005, p. 8-9

Ross, Steven J.; "Instant Mess," *Information Systems Control Journal*, vol. 5, 2004, p. 9-10

Ross, Steven J.; "Mahogany Row Mail Call," *Information Systems Control Journal*, vol. 3, 2001, p. 9-10

Ross, Steven; "Penetrating Questions," *Information Systems Control Journal*, vol. 4, 2001, p. 11-12

Ross, Steven J.; "Standard Questions," *Information Systems Control Journal*, vol. 2, 2001, p. 11-12

Ross, Steven J.; "Why Passwords Persist," *Information Systems Control Journal*, vol. 1, 2001, p. 13-14

Sarup, Deepak; "Watchdog or Bloodhound? The Push and Pull Toward a New Audit Model," *Information Systems Control Journal*, vol. 1, 2004, p. 23-26

Sarup, Deepak; "Surfing @ the Razor's Edge: Governance and Managing Change," *Information Systems Control Journal*, vol. 6, 2002, p. 17-19

Sayana, S. Anantha; "Auditing Business Continuity," *Information Systems Control Journal*, vol. 1, 2005, p. 11-13

Sayana, S. Anantha; "Auditing IT Service Delivery," *Information Systems Control Journal*, vol. 5, 2005, p. 13-14

Sayana, S. Anantha; "Audit of Outsourcing," *Information Systems Control Journal*, vol. 5, 2004, p. 11-13

Sayana, S. Anantha; "Using CAATs to Support IS Audit," *Information Systems Control Journal*, vol. 1, 2003, p. 21-23

Scammell, Tim; "Security Architecture: One Practitioner's View," *Information Systems Control Journal*, vol. 1, 2003, p. 24-28

Schneier, Bruce; *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, 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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Schreider, Tari; "Privacy Is in the Eye of the Beholder," *Information Systems Control Journal*, vol. 6, 2003, p. 46-48

Schreider, Tari; "Risk Assessment Tools: A Primer," *Information Systems Control Journal*, vol. 2, 2003, p. 23-25

Sethi, V.; W.R. King; *Introduction to BPR*, 1988

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

Shue, Lily; "Sarbanes-Oxley and IT Outsourcing," *Information Systems Control Journal*, vol. 5, 2004, p. 28-30

Shue, Lily; "The Global Status of Electronic Signature Legislation," *Information Systems Control Journal*, vol. 5, 2002, p. 24-26

Shue, Lily; "Virtual Private Networking—New Issues for Network Security," *Information Systems Control Journal*, vol. 1, 2001, p. 20-21

Software Engineering Institute, "Spiral Development: Experiences, Principles and Refinements," Special Report CMU/SEI-2000-SR-008, Spiral Development Workshop, 9 February 2000

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

Sparks, Harry A.; "Getting Action on Audit Results," *Information Systems Control Journal*, vol. 6, 2003, p. 37-40

Srinivas, Sarva; "Cost-effective Implementation of Identity Management," *Information Systems Control Journal*, vol. 1, 2005, p. 49-50

Srinivas, Sarva; "Road Map to XBRL Adoption as New Reporting Model," *Information Systems Control Journal*, vol. 1, 2004, p. 50-51

Srinivasan, S.; Alan S. Levitan; "Secure and Practical Smart Card Applications," *Information Systems Control Journal*, vol. 5, 2003, p. 27-30

Standards Australia and Standards New Zealand Technical Committee; The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:1990

Stanley, Richard A.; "Security, Audit and Control Issues for Managing Risk in the Wireless LAN Environment," *Information Systems Control Journal*, vol. 3, 2004, p. 23-25

Stanley, Richard A.; "Wireless LAN Risk and Vulnerabilities," *Information Systems Control Journal*, vol. 2, 2002, p. 57-61

Stasiak, Ken; "Web Application Security," *Information Systems Control Journal*, vol. 6, 2002, p. 44-46

Stein, Douglas M; Vairam Arunachalam; Larry E. Rittenberg; "Electronic Commerce System Sophistication and the Audit Process: Insights from Information Systems Auditors," *Information Systems Control Journal*, vol. 1, 2001, p. 33-38

Stephenson, Peter; *Investigating Computer-related Crime*, CRC Press, USA, 2000

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (continued)

Steuperaert, Dirk; "IT Governance Global Status Report," *Information Systems Control Journal*, vol. 5, 2004, p. 24-26

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

Taylor & Francis Group, "International Journal of Computer Integrated Manufacturing," USA, 2004, www.tandf.co.uk/journals/titles/0951192X.asp

Taylor, Patrick; "A Wake Up Call to All Information Security and Audit Executives: Become Business-relevant," *Information Systems Control Journal*, vol. 6, 2004, p. 48-50

Telford, Thomas; Loftus, J. (Ed), *Project Management of Multiple Projects and Contracts*, 1999

Thorp, Carl; "Implementing ISO 17799: Pleasure or Pain?," *Information Systems Control Journal*, vol. 4, 2004, p. 25-26

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

Tongia, Rahul; Kanika Jain; "Investing in Security—Do Not Rely on FUD," *Information Systems Control Journal*, vol. 6, 2003, p. 27-28

Trustweaver, "Legal Aspects of PKI: Fact sheet," 31 August 2004, www.tekki.se/docs/lbwp.pdf

Tschanz, David W.; "Stop Spam Now," RedmondMag.com, 2005, www.cmsconnect.com/News/CMSInPrint/Redmond-050302.htm

University of New Haven Center for Cybercrime and Forensic Computer Investigation and the University of Southern California Department of Mathematics; "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security," *Information Systems Control Journal*, vol. 2, 2001, p. 32-34

Unwala, Huzeifa; "Return on Information Technology," *Information Systems Control Journal*, vol. 2, 2004, p. 51-53

Van Grembergen, Wim; Steven De Haes; "Measuring and Improving IT Governance Through the Balanced Scorecard," *Information Systems Control Journal*, vol. 2, 2005, p. 35-42

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

Wakefield, Robin L.; "Employee Monitoring and Surveillance—The Growing Trend," *Information Systems Control Journal*, vol. 1, 2004, p. 47-49

Wakefield, Robin; "Auditor Due Care in E-commerce," *Information Systems Control Journal*, vol. 5, 2002, p. 41-42

Walker, Tony; "Fighting Security Breaches and Cyberattacks With Two-factor Authentication Technology," *Information Systems Control Journal*, vol. 2, 2001, p. 41-42

Wallhoff, John; "Enforce Security With a Fingerprint Biometric Solution," *Information Systems Control Journal*, vol. 4, 2003 p. 39-43

Wang, George; "Strategies and Influence for Information Security," *Information Systems Control Journal*, vol. 1, 2005, www.isaca.org/jonline

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

Reference Materials (*continued*)

Wikimedia Foundation; "ACID (Atomicity, Consistency, Isolation and Durability)," *Wikipedia*, www.wikipedia.org/wiki/ACID

Wikimedia Foundation; "Artificial Intelligence," *Wikipedia*, http://en.wikipedia.org/wiki/Artificial_intelligence

Wikipedia, www.wikipedia.com

Wilkins, Adam; "E-mail Records and Knowledge Management: The Hidden Risk," *Information Systems Control Journal*, vol. 4, 2002, p. 25-27

Williams, Paul; "Continuous Auditing: Is It Fantasy or Reality?," *Information Systems Control Journal*, vol. 5, 2002, p. 43-46

Williams, Paul; "Optimising Returns From IT-related Business Investments," *Information Systems Control Journal*, vol. 5, 2005, p. 41-45

Willoughby, Mark K.; "Automated User Authentication: The Final Frontier of Information Security," *Information Systems Control Journal*, vol. 2, 2001, p. 21-23

Woda, Alex; "The Role of the Auditor in IT Governance," *Information Systems Control Journal*, vol. 2, 2002, p. 18-20

Woodward, John D.; "Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint," *University of Pittsburgh Law Review*, USA, 1997, www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf

Wright, Benjamin; "The Cost of Not Securing Personally Identifiable Data," *Information Systems Control Journal*, vol. 4, 2004, p. 21-22

Wright, Catherine; "Top Three Potential Risks With Outsourcing Information Systems," *Information Systems Control Journal*, vol. 5, 2004, p. 40-42

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 articles are available on the CISA CD-ROM 2006. For references by content area, please refer to ISACA CISA Review Manual.

Candidate's Guide to the CISA Exam

List of Acronyms

The CISA candidate should be familiar with the following list of acronyms published in the *Candidate's Guide to the CISA Examination*. These acronyms are the only stand-alone abbreviations permitted to be used in examination questions.

ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode or automated teller machine
Bit	Binary digit
CASE	Computer-aided system engineering
CPM	Critical path method
CPU	Central processing unit
CSF	Critical Success Factors
DASD	Direct Access Storage Device
DBA	Database administrator
DBMS	Database management system
DES	Data Encryption Standard
EDI	Electronic data interchange
EFT	Electronic funds transfer
EIGRP	Enhanced Interior Gateway Routing Protocol
EMRT	Emergency response time
FTP	File Transfer Protocol
I/O	Input/output
IP	Internet protocol
IPL	Initial program load
IS	Information systems
ISAM	Indexed Sequential Access Method
ISDN	Integrated services digital network
ISO	International Organization for Standardization
ISP	Internet service provider
ITF	Integrated test facility
KGI	Key goal indicators
KPI	Key performance indicators
LAN	Local area network
MODEM	Modulator/demodulator
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PBX	Private branch exchange
PC	Personal computer/microcomputer
PDA	Personal digital assistant
PERT	Program evaluation review technique
PKI	Public key infrastructure
QA	Quality assurance
RAM	Random access memory
ROM	Read-only memory
SMART	Specific, Measurable, Achievable, Relevant, Time-bound
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TQM	Total quality management
UPS	Uninterruptible power supply
USB	Universal Serial BUS
WAN	Wide area network

Candidate's Guide to the CISA Exam

List of Acronyms (*continued*)

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 examination questions, their meanings would be included when the acronym appears.

AICPA	American Institute of Certified Public Accountants	IRC	Internet relay chat
ALU	Arithmetic logic unit	L2TP	Layer 2 Tunneling Protocol
API	Application programming interface	MAC	Media Access Control
BCP	Business continuity planning	MIS	Management information system
BIA	Business impact analysis	MSAUs	Multistation access units
BLP	Bypass label process	NAT	Network address translation
BPR	Business process reengineering	NFS	Network files system
CA	Certificate authority	NNTP	Network News Transfer Protocol
CAAT	Computer-assisted audit technique	NTP	Network Time Protocol
CEO	Chief executive officer	PAD	Packet assembler/disassembler
COBIT	<i>Control Objectives for Information and related Technology</i>	PCR	Program change request
CGI	Common gateway interface	PID	Process ID
CICA	Canadian Institute of Chartered Accountants	PIN	Personal identification number
CIS	Continuous and intermittent simulation	PPPoE	Point-to-point Protocol Over Ethernet
CPS	Certificate practice statement	POS	Point of sale
CRL	Certificate revocation list	PPP	Point-to-point Protocol
CRM	Customer relationship management	RA	Registration authority
CSF	Critical success factor	RAID	Redundant Array of Inexpensive Disks
CSMA/CD	Carrier-sense Multiple Access/Collision Detection	RAS	Remote access service
DCE	Data communications equipment	RDBMS	Relational database management system
DCE	Distributed computing environment	RFI	Request for information
DID	Direct inward dial	RFP	Request for proposal
DNS	Domain name server	SCM	Supply chain management
DRP	Disaster recovery planning	SDLC	System development life cycle
DSS	Decision support systems	SET	Secure electronic transactions
EC	Electronic commerce	SNMP	Simple Network Management Protocol
ERP	Enterprise resource management	SPOOL	Simultaneous peripheral operations online
FAT	File allocation table	SQL	Structured Query Language
FRAD	Frame relay assembler/disassembler	TCP/IP	Transmission Control Protocol/Internet Protocol
GID	Group ID	TMS	Tape management system
HIPO	Hierarchy Input-Process-Output	UBE	Unsolicited bulk e-mail
HTML	Hypertext Markup Language	UDP	User Datagram Protocol
HTTP	Hypertext Transmission Protocol	UID	User ID
ID	Identification	URL	Universal resource locator
IETF	Internet engineering task force	VAN	Value-added network
IPF	Information processing facility	VPN	Virtual private network
		WWW	World Wide Web
		XML	Extensible Markup Language

Candidate's Guide to the CISA Exam

Sample Admission Ticket

The following is a sample of the admission ticket that you will receive approximately two to three weeks prior to the CISA examination date (see page 4).

Professional Examination Service

You are scheduled to take the ISACA Certified Information Systems Auditor™ (CISA®) Examination on Saturday, 10 June 2006. Report no later than xx:xx a.m. on the morning of the examination to the test site listed below. The Chief Examiner will begin reading the instructions at xx:xx a.m.

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 his or her registration fee. To ensure that you arrive in plenty of time for the examination, it is recommended that you become familiar with the exact location of your exam site and the best route to get there. Test center phone numbers and web site references have been provided (when available) to assist you in obtaining directions to the facility.

The timed portion of the examination is four (4) hours from xx:xx a.m. to xx:xx p.m.

TEST SITE CODE #
Test Site Name
Street Address
City, State, Postal Code or Zip Code
Country
Website or Direction Information, if available

Your Identification Number is NNNNNNNN
You are scheduled for the xxxxxx language version of the exam

YOU MUST bring your exam admission ticket (e-ticket or ticket received in the mail), several sharpened No. 2 or HB pencils, an eraser and an original, acceptable form of identification (such as a driver's license or passport) to the test site. Any candidate who does not provide an original form of identification will not be allowed to sit for the exam and will forfeit his or her registration fee. Please retain this admission ticket for future reference.

If you have any questions, please contact ISACA at +1.847.253.1545, extension 403, 471 or 474, or via e-mail at: certification@isaca.org.

PROFESSIONAL EXAMINATION SERVICE

ISACA

Test date: Saturday, 10 June 2006: 7401

CHANGE of NAME/ADDRESS/ID# FORM

Please print clearly any change or correction to your NAME, ADDRESS or ID# on this form and return this part of the form to your exam proctor when instructed to do so. **DO NOT** return this part of the form if there are no changes to be recorded.

ID #: NNNNNNNN

Name:

Address 1:

Address 2:

City, State, Country, Postal Code or Zip Code:

Candidate's Guide to the CISA Exam

Sample Answers Sheet (Side 2)

The following is a sample of a CISA exam answer sheet.

YOUR SIGNATURE/SEAL REQUIRED HERE: _____

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

Mark Reader® by NCS EM-238649-1-654321

HR04

Printed in U.S.A.

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

SAMPLE

Chicago is:

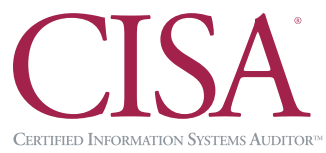
1. a country
2. a mountain
3. an Island
4. a city

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

www.isaca.org