

# CISM<sup>®</sup>

CERTIFIED INFORMATION  
SECURITY MANAGER<sup>®</sup>

## 2006 Candidate's Guide to the CISM 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

# Candidate's Guide to the CISM Exam

---

## Reference Materials

### 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 CISM Certification Board have designed the *Candidate's Guide to the CISM Exam* as a guide to those pursuing the CISM 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 CISM exam.

### Disclosure

Copyright © 2006 by ISACA. Reproduction or storage in any form for any purpose is not permitted without prior written permission from ISACA. 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](mailto:certification@isaca.org)

Web site: [www.isaca.org](http://www.isaca.org)

ISBN 1-933284-36-6

*Candidate's Guide to the CISM Exam*

Printed in the United States of America

## Table of Contents

<b>Introduction</b> . . . . .	<b>.2</b>
<b>Recognition as a CISM</b> . . . . .	<b>.2</b>
<b>Recognition for Other Security Certifications Earned</b> . . . . .	<b>.2</b>
<b>Worldwide Recognition</b> . . . . .	<b>.2</b>
<b>CISM Program Receives ANSI Accreditation</b> . . . . .	<b>.2</b>
<b>The CISM Exam</b> . . . . .	<b>.3</b>
<b>Types of Questions on the CISM Exam</b> . . . . .	<b>.3</b>
<b>Study Aids for the CISM Exam</b> . . . . .	<b>.4</b>
<b>Administration of the CISM Exam</b> . . . . .	<b>.5</b>
<b>Scoring the CISM Exam</b> . . . . .	<b>.7</b>
<b>Application for CISM Certification</b> . . . . .	<b>.7</b>
<b>Requirements for Maintaining CISM Certification</b> . . . . .	<b>.8</b>
<b>Revocation of CISM Certification</b> . . . . .	<b>.8</b>
<b>ISACA Code of Professional Ethics</b> . . . . .	<b>.9</b>
<b>Content of the CISM Exam</b> . . . . .	<b>.9</b>
<b>Reference Materials</b> . . . . .	<b>.14</b>
<b>Sample Admission Ticket</b> . . . . .	<b>.18</b>
<b>Sample Answer Sheet</b> . . . . .	<b>.19</b>

# Candidate's Guide to the CISM Exam

---

## Introduction

The Certified Information Security Manager® (CISM®) certification program is developed specifically for experienced information security managers and those who have information security management responsibilities.

The CISM certification is for the individual who manages, designs and oversees an enterprise's information security. While its central focus is security management, all those in the IS profession with security experience will find value the CISM credential. The CISM certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services. Individuals earning the CISM certification become part of an elite peer network, attaining a one-of-a-kind credential. The CISM job practice also defines a global job description for the information security manager and a method to measure existing staff or compare prospective new hires.

## Recognition as an Information Security Manager

CISM is unique in the information security credential marketplace because it is designed specifically and exclusively for individuals who have experience managing an information security program. Requirements to become a CISM are based on the experience necessary to competently perform the duties and responsibilities of an information security manager. Information security leaders, subject matter experts and practicing information security managers developed these requirements and the knowledge that is measured through the exam. The results are an information security credential designed to measure an individual's management experience in information security situations, not general practitioner skills.

## Recognition for Other Security Certifications Earned

CISM is for the individual who must manage and oversee the enterprise's information security effort, many of whom may hold other certifications the field offers. CISM provides the information security professional with an opportunity to build upon existing credentials already earned and provides tangible evidence of career growth. The CISM certification program recognizes the achievement of security credentials as baseline representations that an individual has gained general information security skill and knowledge. Information security professionals that have earned credentials such as the Certified Information Systems Auditor™ (CISA®), Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+ and the Certified Business Continuity Professional (CBCP), to name a few, are eligible for general information security experience requirement waivers.

## Worldwide Recognition

Although certification may not be mandatory for you at this time, a growing number of organizations are requiring or recommending that employees become certified. To help ensure success in the global marketplace, it is vital to select a certification program based on universally accepted information security management practices. CISM delivers such a program.

## CISM Program Accredited Under ISO/IEC 17024:2003

The American National Standards Institute (ANSI) has accredited the CISM 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's 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 CISM and CISA will continue to present themselves around the world.

# Candidate's Guide to the CISM Exam

---

## The CISM Exam

### Development/Description of the CISM Exam

The detailed job practice areas (see the Content of the CISM Exam Section on page 9) serve as a syllabus for the CISM exam. These tasks and knowledge statements were developed by the CISM Certification Board, validated by subject matter experts, and serve as the blueprint for the CISM exam content and emphasis. They are intended to be a comprehensive list of tasks performed by information security managers and the knowledge needed to perform these tasks.

The CISM Certification Board oversees the development of the exam and ensures the currency of its content. The exam consists of 200 questions administered annually in June and December during a four-hour session. Questions for the CISM exam are developed through a comprehensive process designed to ensure the ultimate quality of the exam.

### 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](http://www.isaca.org/examdefer). NO REFUNDS OR EXCHANGES WILL BE GIVEN FOR STUDY AIDS, ASSOCIATED TAXES, SHIPPING AND HANDLING CHARGES OR MEMBERSHIP FEES.

## Types of Questions on the CISM Exam

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

Every CISM exam 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 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 CISM 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.

### 1. When a security standard conflicts with a business objective, the situation should be resolved by:

- A. changing the security standard.
- B. enforcing the security standard.
- C. **performing a risk analysis.**
- D. allowing an exception to the standard.

### 2. During which phase of development is it **MOST** appropriate to begin assessing the risk of a new application system?

- A. **Feasibility**
- B. Design
- C. Development
- D. Testing

# Candidate's Guide to the CISM Exam

---

3. Which of the following is the **MOST** effective in preventing attacks that exploit weaknesses in operating systems?
- A. **Patch management**
  - B. Change management
  - C. Security baselines
  - D. Acquisition management
4. Which of the following environments would be the **MOST** likely to deviate from organizational security policies?
- A. Locally managed file server
  - B. Enterprise data warehouse
  - C. Load-balanced, web server cluster
  - D. Centrally managed data switch
5. An organization with multiple data centers has terminated its external hot site contract and has designated one of its own data centers as the recovery site. The **MOST** important concern is the:
- A. communication line capacity between data centers.
  - B. **current processing capacity loads at data centers.**
  - C. differences in logical and physical security at each center.
  - D. synchronization of system software release versions.

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 *CISM Questions, Answers & Explanations Manual*.

## Study Aids for the CISM Exam

Passing the CISM 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/cismexam](http://www.isaca.org/cismexam) for more details).

- The *Candidate's Guide to the CISM Exam* is supplied to individuals upon receipt of the CISM exam registration form and payment. This guide provides general information regarding the administration of the exam as well as a detailed outline of the job practice areas, task statements and knowledge statements covered on the exam and a sample copy of the exam answer sheet.
- *CISM Review Manual 2006* is a reference guide designed to assist individuals in preparing for the CISM examination and for individuals wanting to learn more about the role and responsibilities of an information security manager. The 2006 edition is significantly enhanced with changes of structure for a more comprehensive flow, updates to the content reflecting regulatory and technical changes, and expanded coverage of critical areas. The manual features detailed descriptions of the tasks performed by information security managers and the knowledge necessary to manage, design and oversee an enterprise's information security program. These task and knowledge statements were developed by the CISM Certification Board, validated by subject matter experts, and serve as the blueprint for the CISM examination content and emphasis. Information provided includes applicable information security management principles, practices and strategies. Detailed references of where to find additional guidance materials are also provided. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and review courses. The *CISM Review Manual 2006* also provides definitions and practical examples to facilitate the learning process. **(CM-6)**
- *CISM Questions, Answers & Explanations Manual 2006* consists of 200 multiple-choice study questions arranged in the same proportion as the CISM job areas. These items appeared in the 2004 and 2005 editions of the *CISM Review Questions, Answers & Explanations Manual*, but have been combined into one manual. These questions are not actual exam items, and are intended to provide the CISM candidate with an understanding of the type and structure of questions and subject matter that has previously appeared on the examination. Items are also provided in a random order as a practice exam. This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*. **(CQA-6)**

# Candidate's Guide to the CISM Exam

---

- *CISM Questions, Answers and Explanations Manual 2006 Supplement* consists of 100 multiple-choice study questions arranged in the same proportion as the CISM job practice areas. The questions include answers and detailed explanations for the candidates to use in preparation for the CISM exam. Unlike some review manuals that use questions from other certification exams, these questions were prepared especially for use in studying for the CISM exam. These questions are intended to provide the CISM candidate with an understanding of the type and structure of questions that have typically appeared on the examination and are not actual test items. This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006*. **(CQA-6ES)**
- CISM review courses are conducted by many ISACA chapters. Exam candidates should contact their local ISACA chapter(s) to find out if a review course is being offered. Information pertaining to chapter contacts and course offerings are available at [www.isaca.org/chapters](http://www.isaca.org/chapters) and [www.isaca.org/cismexam](http://www.isaca.org/cismexam), respectively.

The 2005 editions of the CISM study aids are available in Japanese and Spanish and can be used to prepare for the 2006 CISM exam. Please see [www.isaca.org/nonenglishbooks](http://www.isaca.org/nonenglishbooks) for details.

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

## Administration of the CISM 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 CISM exam.

### Admission Ticket

Approximately two to three weeks prior to the CISM 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 CISM 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](mailto: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 begin will not be allowed to sit for the exam and will forfeit his or her registration fees. 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 CISM certification department immediately at [certification@isaca.org](mailto: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 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 original 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. To be admitted, a candidate must also present a valid admission ticket or other evidence indicating to the testing agency representative that admission should be granted.

# Candidate's Guide to the CISM Exam

---

## Observe the Test Center's Rules

- Candidates will not be admitted to a testing room after the reading of the oral instructions has 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 device (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.

## Be Careful in Completing the Answer Sheet

- An example of the multiple-choice answer sheet is included to familiarize candidates with its format.
- Before a candidate begins the exam, the test center chief examiner will read aloud the instructions for entering identification information on the answer sheet. A candidate's identification number as it appears on the admission ticket and all other requested information must be entered correctly or scores may be delayed or reported incorrectly.
- 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.
- The exam consists of 200 multiple-choice questions. All answers are to be marked in the appropriate circle on the answer sheet. Candidates must be careful to mark no more than one answer per question and to be sure to answer a question in the appropriate row of answers. If an answer needs to be changed, a candidate is urged to fully erase the wrong answer before marking in the new one.
- All questions should be answered. **There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly; so do not leave any questions blank.**
- After completion, candidates are required to hand in their answer sheet and test booklet.

## Budget 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 CISM 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 CISM 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.

# Candidate's Guide to the CISM Exam

---

## Scoring the CISM Exam

The CISM 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 will be 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 flaws will either not be used in the grading process or will be given multiple correct answer keys. Raw scores then will be mathematically converted to scaled scores. A scaled score of 75 or above represents a passing score for the entire exam.

**Test scores will not be available until approximately six (6) weeks after the test date. The CISM 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 CISM exam registration form.**

Candidates will receive a score report containing a subscore for each job area. Successful candidates will receive, along with a score report, an application for CISM certification. Unsuccessful candidates will receive, along with a score report, a copy of the new Bulletin of Information. The subscores 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 subscores does not derive the total scaled score.

Candidates receiving a failing score on the exam may request a hand score of their answer sheets. This procedure ensures that no stray marks, multiple responses or other conditions interfered with computer scoring. 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.

## Application for CISM Certification

Passing the exam does not mean a candidate is a CISM. Once a candidate passes the CISM exam, he or 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 CISM designation, until the completed application is received and approved.** Once certified, the new CISM will receive a certificate and a copy of the CISM Continuing 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 CISM status.

## Requirements for CISM Certification

Certification is granted to individuals who have completed the CISM exam successfully, agree to comply with the CISM Continuing Professional Education Policy, agree to adhere to the ISACA Code of Professional Ethics and meet CISM work experience requirements. These requirements are a minimum of five (5) years of information security work experience, with a minimum of three (3) years of information security management work experience in three or more of the job practice areas. General information security experience substitutions may be obtained. However, there are no substitutions available for information security management experience.

# Candidate's Guide to the CISM Exam

---

## Experience Substitutions

Other security certifications and information systems management experience can be used to satisfy up to two years of general information security work experience.

- Two years may be substituted for the achievement of one of the following:
  - Certified Information Systems Auditor (CISA) in good standing
  - Certified Information Systems Security Professional (CISSP) in good standing
  - Postgraduate degree in information security or a related field (for example, business administration, information systems or information assurance)

OR

- One year may be substituted for the achievement of one of the following:
  - One full year of information systems management experience
  - One full year of general security management experience
  - Skill-based security certification [e.g., SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+, Disaster Recovery Institute Certified Business Continuity Professional (CBCP) or ESL IT Security Manager.]

***The experience substitutions will not satisfy any portion of the three-year information security management work experience requirement.***

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

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

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

## Requirements for Maintaining CISM Certification

The CISM Continuing Education Policy requires the attainment of continuing education hours over an annual and three-year reporting period. CISM holders 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 CISM designation.**

## Revocation of CISM Certification

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

- Failing to comply with the CISM 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 CISM exam or the certification process

# Candidate's Guide to the CISM Exam

---

## ISACA Code of Professional Ethics

The Information Systems Audit and Control Association 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.

## Content of the CISM Exam

ISACA's philosophy toward certification is to measure an individual's ability and knowledge as it pertains to the performance of his or her job. To ensure that the CISM exam is reflective of the work performed by information security managers, a series of tasks and knowledge statements were developed by prominent industry leaders, subject matter experts and industry practitioners. These tasks and knowledge statements were later organized into practice areas and measured and validated through the use of a survey distributed to information security directors, managers and officers. The results serve as the basis for the content for the CISM exam.

**Note:** The percentages below indicate the emphasis or percent of questions that will appear on the CISM 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.

### **Information Security Governance (21%)**

Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

### **Risk Management (21%)**

Identify and manage information security risks to achieve business objectives.

### **Information Security Program Management (21%)**

Design, develop and manage an information security program to implement the information security governance framework.

### **Information Security Management (24%)**

Oversee and direct information security activities to execute the information security program.

### **Response Management (13%)**

Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

# Candidate's Guide to the CISM Exam

<p><b>Information Security Governance</b></p> <p>Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.</p>
<p><b>Tasks</b></p> <p>Develop the information security strategy in support of business strategy and direction.</p> <p>Obtain senior management commitment and support for information security throughout the enterprise.</p> <p>Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.</p> <p>Establish reporting and communication channels that support information security governance activities.</p> <p>Identify current and potential legal and regulatory issues affecting information security and assess their impact on the enterprise.</p> <p>Establish and maintain information security policies that support business goals and objectives.</p> <p>Ensure the development of procedures and guidelines that support information security policies.</p> <p>Develop a business case and enterprise value analysis that support information security program investments.</p>
<p><b>Knowledge Statements</b></p> <p>Knowledge of information security concepts</p> <p>Knowledge of the relationship between information security and business operations</p> <p>Knowledge of techniques used to secure senior management commitment and support of information security management</p> <p>Knowledge of methods of integrating information security governance into the overall enterprise governance framework</p> <p>Knowledge of practices associated with an overall policy directive that captures senior management-level direction and expectations for information security in laying the foundation for information security management within an organization</p> <p>Knowledge of an information security steering group function</p> <p>Knowledge of information security management roles, responsibilities and organizational structure</p> <p>Knowledge of areas of governance (e.g., risk management, data classification management, network security and systems access)</p> <p>Knowledge of centralized and decentralized approaches to coordinating information security</p> <p>Knowledge of legal and regulatory issues associated with Internet businesses, global transmissions and transborder data flows (e.g., privacy, tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets and national security)</p> <p>Knowledge of common insurance policies and imposed conditions (e.g., crime or fidelity insurance and business interruptions)</p> <p>Knowledge of the requirements for the content and retention of business records and compliance</p> <p>Knowledge of the process for linking policies to enterprise business objectives</p> <p>Knowledge of the function and content of essential elements of an information security program (e.g., policy statements, procedures and guidelines)</p> <p>Knowledge of techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures</p> <p>Knowledge of information security process improvement and its relationship to traditional process management</p> <p>Knowledge of information security process improvement and its relationship to security architecture development and modeling</p> <p>Knowledge of information security process improvement and its relationship to security infrastructure</p> <p>Knowledge of generally accepted international standards for information security management and related process improvement models</p> <p>Knowledge of the key components of cost-benefit analysis and enterprise transformation/migration plans (e.g., architectural alignment, organizational positioning, change management, benchmarking and market/competitive analysis)</p> <p>Knowledge of a methodology for business case development and computing enterprise value proposition</p>

# Candidate's Guide to the CISM Exam

<b>Risk Management</b>
Identify and manage information security risks to achieve business objectives.
<b>Tasks</b>
Develop a systematic, analytical and continuous risk management process.
Ensure that risk identification, analysis and mitigation activities are integrated into life cycle processes.
Apply risk identification and analysis methods.
Define strategies and prioritize options to mitigate risk to levels acceptable to the enterprise.
Report significant changes in risk to appropriate levels of management on both a periodic and event-driven basis.
<b>Knowledge Statements</b>
Knowledge of information resources used in support of business processes
Knowledge of information resource valuation methodologies
Knowledge of information classification
Knowledge of the principles of development of baselines and their relationship to risk-based assessments of control requirements
Knowledge of life cycle-based risk management principles and practices
Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources
Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events
Knowledge of use of gap analysis to assess generally accepted standards of good practice for information security management against the current state
Knowledge of recovery time objectives (RTOs) for information resources and how to determine RTO
Knowledge of RTO and its relation to business continuity and contingency planning objectives and processes
Knowledge of risk mitigation strategies used in defining security requirements for information resources supporting business applications
Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks, threats and exposures to acceptable levels
Knowledge of managing and reporting status of identified risks

<b>Information Security Program Management</b>
Design, develop and manage an information security program to implement the information security governance framework.
<b>Tasks</b>
Create and maintain plans to implement the information security governance framework.
Develop information security baseline(s).
Develop procedures and guidelines to ensure business processes address information security risk.
Develop procedures and guidelines for IT infrastructure activities to ensure compliance with information security policies.
Integrate information security program requirements into the organization's life cycle activities.
Develop methods of meeting information security policy requirements that recognize impact on end users.
Promote accountability by business process owners and other stakeholders in managing information security risks.
Establish metrics to manage the information security governance framework.
Ensure that internal and external resources for information security are identified, appropriated and managed.

# Candidate's Guide to the CISM Exam

<b>Information Security Program Management (continued)</b>
<b><i>Knowledge Statements</i></b>
Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analyses
Knowledge of project management methods and techniques
Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and levels of the enterprise
Knowledge of security baselines and configuration management in the design and management of business applications and the infrastructure
Knowledge of information security architectures (e.g., single sign-on, rules-based as opposed to list-based system access control for systems and limited points of systems administration)
Knowledge of information security technologies (e.g., cryptographic techniques and digital signatures) to enable management to select appropriate controls
Knowledge of security procedures and guidelines for business processes and infrastructure activities
Knowledge of the systems development life cycle methodologies (e.g., traditional SDLC and prototyping)
Knowledge of planning, conducting, reporting and follow-up of security testing
Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework
Knowledge of types, benefits and costs of physical, administrative and technical controls
Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes
Knowledge of security metrics design, development and implementation
Knowledge of acquisition management methods and techniques (e.g., evaluation of vendor service level agreements, and preparation of contracts)

<b>Information Security Management</b>
Oversee and direct information security activities to execute the information security program.
<b><i>Tasks</i></b>
Ensure that the rules of use for information systems comply with the enterprise's information security policies.
Ensure that the administrative procedures for information systems comply with the enterprise's information security policies.
Ensure that services provided by other enterprises, including outsourced providers, are consistent with established information security policies.
Use metrics to measure, monitor and report on the effectiveness and efficiency of information security controls and the compliance with information security policies.
Ensure that information security is not compromised throughout the change management process.
Ensure that vulnerability assessments are performed to evaluate the effectiveness of existing controls.
Ensure that noncompliance issues and other variances are resolved in a timely manner.
Ensure the development and delivery of activities that can influence the culture and behavior of staff, including information security education and awareness.
<b><i>Knowledge Statements</i></b>
Knowledge of how to interpret information security policies into operational use
Knowledge of information security administration process and procedures
Knowledge of methods for managing the implementation of the enterprise's information security program through third parties, including trading partners and security service providers

# Candidate's Guide to the CISM Exam

<b>Information Security Management (continued)</b>
Knowledge of continuous monitoring of security activities in the enterprise's infrastructure and business applications
Knowledge of methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators
Knowledge of change and configuration management activities
Knowledge of information security management due diligence activities and reviews of the infrastructure
Knowledge of liaison activities with internal/external assurance providers performing information security reviews
Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information resources
Knowledge of external vulnerability reporting sources that provide information that may require changes to the information security in applications and infrastructure
Knowledge of events affecting security baselines that may require risk reassessments and changes to information security requirements in security plans, test plans and reperformance
Knowledge of information security problem management practices
Knowledge of information security manager facilitative roles as change agents, educators and consultants
Knowledge of the ways in which culture and cultural differences affect the behavior of staff
Knowledge of activities that can change the culture and behavior of staff
Knowledge of methods and techniques for security awareness training and education

<b>Response Management</b>
Develop and manage a capability to respond to and recover from disruptive and destructive information security events.
<b>Tasks</b>
Develop and implement processes for detecting, identifying and analyzing security-related events.
Develop response and recovery plans that include organizing, training and equipping the teams.
Ensure periodic testing of the response and recovery plans, where appropriate.
Ensure the execution of response and recovery plans, as required.
Establish procedures for documenting an event as a basis for subsequent action, including forensics, when necessary.
Manage post-event reviews to identify causes and corrective actions.
<b>Knowledge Statements</b>
Knowledge of the components of an incident response capability
Knowledge of information security emergency management practices (e.g., production change control activities and development of a computer emergency response team)
Knowledge of disaster recovery planning and business recovery processes
Knowledge of disaster recovery testing for infrastructure and critical business applications
Knowledge of escalation processes for effective security management
Knowledge of intrusion detection policies and processes
Knowledge of help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with by the help desks
Knowledge of the notification process in managing security incidents and recovery (e.g., automated notice and recovery mechanisms in response to virus alerts in a real-time fashion)
Knowledge of the requirements for collecting and presenting evidence, rules for evidence, admissibility of evidence, and quality and completeness of evidence
Knowledge of post-incident reviews and follow-up procedures

# Candidate's Guide to the CISM Exam

---

## Reference Materials Information Security Governance

Andriole, Steve; "8 Keys to a Sane Security Strategy," *Datamation*, 31 July 2001

Information Systems Audit and Control Association, "IS Standards, Guidelines and Procedures for Auditing and Control Professionals," 2004, [www.isaca.org](http://www.isaca.org)

*Information Systems Control Journal*, ISACA, USA:

"Cross-border Privacy Impact Assessments: An Introduction," Volume 3, 2001, p. 50-52

"Insuring Information Security: Commercial Insurance as an Information Security Driver," Volume 1, 2002, p. 44-47

"Make Sure Management and IT Are on the Same Page: Implementing an IT Governance Framework," Volume 3, 2002, p. 14-16

"Surfing @ the Razor's Edge: Governance and Managing Change," Volume 6, 2002, p. 17-19

International Federation of Accountants, *Managing Security of Information*, 1998

IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, 3<sup>rd</sup> Edition, Rolling Meadows, Illinois, USA, 2000, [www.isaca.org](http://www.isaca.org)

IT Governance Institute, [www.itgi.org](http://www.itgi.org)

IT Governance Institute, *Board Briefing on IT Governance* 2<sup>nd</sup> Edition, Rolling Meadows, Illinois, USA, 2003, [www.itgi.org](http://www.itgi.org)

IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, Rolling Meadows, Illinois, USA, 2001, [www.itgi.org](http://www.itgi.org)

Peltier, Thomas R.; *Information Security Policies and Procedures: A Practitioners Reference* 2<sup>nd</sup> Edition, Auerbach, 2004

Wood, Charles Cresson; *Information Security Policies Made Easy*, Information Shield, 2005

## Risk Management

*Information Systems Control Journal*, ISACA, USA:

"Erosion of Trust—E-commerce and the Loss of Privacy," Volume 3, 2001, p. 46-49

"The State of Enterprise Security Management," Volume 6, 2001, p. 38-40

"Risk Management for Internet Banking," Volume 6, 2001, p. 48-50

"New Basel Accord: Operational Risk Management—Emerging Frontiers for the Profession," Volume 1, 2002, p. 37-42

"Risk Management in IT Projects," Volume 5, 2002, p. 37-39

"An Exploration of Global Perceptions of Security and Privacy," Volume 6, 2002, p. 27-30

"Risk Assessment Tools: A Primer," Volume 2, 2003, p. 23-25

"Risk-aware Decision Making for New IT Investments," Volume 2, 2003, p. 12-14

"Justifying Investment in Security," Volume 4, 2003, p. 53-55

IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, 3<sup>rd</sup> Edition, Rolling Meadows, Illinois, USA, 2000, [www.isaca.org](http://www.isaca.org)

Joint Australia/New Zealand Standard AS/NZS 4360:1999, Risk Management, 1999

McNamee, David; *Business Risk Assessment*, The Institute of Internal Auditors, USA, 1998

McNamee, David; Joseph R. Pleier; Dr. John D. Tongren; *Risk Management: Best Practice* (CD-ROM only), 1999

Note: Publications in bold are available in the ISACA Bookstore, [www.isaca.org/bookstore](http://www.isaca.org/bookstore)

# Candidate's Guide to the CISM Exam

---

## Risk Management (continued)

Peltier, Thomas R.; *Information Security Risk Analysis*, Auerbach, USA, 2001

Roper, Carl; *Risk Management for Security Professionals*, Butterworth-Heinemann, USA, 1999

## Information Security Program Management

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

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

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

**Blake-Wilson, Simon; John Mitchell; Fred Piper; *Digital Signatures—Security and Controls*, IT Governance Institute, USA, 1999**

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

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

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

Dietel, Harvey M.; *Introduction to Operating Systems*, 2<sup>nd</sup> Edition, Addison-Wesley, 1990

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

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

**Ghosh, Anup K.; *e-Commerce Security: Weak Links, Best Defenses*, John Wiley & Sons Inc., USA, 1998**

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

GTE/BBN Technologies, RFC 2828 Internet Security Glossary, May 2000

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

*Information Systems Control Journal*, ISACA, USA:

**"Why Passwords Persist," Volume 1, 2001, p. 13-14**

**"Virtual Private Networking—New Issues for Network Security," Volume 1, 2001, p. 20-21**

**"Helping Businesses Safeguard Information and Networks," Volume 1, 2001, p. 23**

**"Standard Questions," Volume 2, 2001, p. 11-12**

**"Automated User Authentication: The Final Frontier of Information Security," Volume 2, 2001, p. 21-23**

**"Computer Forensics—From Cottage Industry to Standard Practice," Volume 2, 2001, p. 25-27**

**"Cybersecurity and the Future of E-commerce: The Role of the Audit Community," Volume 2, 2001, p. 29-30**

**"Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security," Volume 2, 2001, p. 32-34**

**"Securing Emerging Internet Applications," Volume 2, 2001, p. 36-39**

# Candidate's Guide to the CISM Exam

---

## Information Security Program Management (continued)

“Fighting Security Breaches and Cyberattacks With Two-Factor Authentication Technology,” Volume 2, 2001, p. 41-42

“Virtual Private Network: Confidentiality on Public Network,” Volume 3, 2001, p. 23-26

“E-commerce and Smart Cards,” Volume 3, 2001, p. 57-58

“Comercio Electrónico y Tarjetas Inteligentes,” Volume 3, 2001, p. 59-60 (Spanish)

“Managing Data Integrity and Accuracy Effectively: The Case for Analysis Software,” Volume 5, 2001, p. 30-32

“Mahogany Row Mail Call,” Volume 3, 2001, p. 9-10

“Virtual Private Networking: Confidentiality on Public Networks,” Volume 3, 2001, p. 23-26

“Top US Privacy Stories of 2000,” Volume 3, 2001, p. 29-31

“Choosing the Best Solution for Your Network Security: Secure Shell, TLS or IPSec,” Volume 3, 2001, p. 33-39

“Penetrating Questions,” Volume 4, 2001, p. 11-12

“Ports and Port Scanning: An Introduction,” Volume 5, 2001, p. 34-39

“Intrusion, Attack, Penetration-Some Issues,” Volume 6, 2001, p. 52-57

“Increasing Security Levels,” Volume 2, 2002, p. 35-41

“Wireless LAN Risk and Vulnerabilities,” Volume 2, 2002, p. 57-61

“Combating Cyberthreats—Partnership Between Public and Private Entities,” Volume 3, 2002, p. 38-43

“New Opportunities for Information System Auditors: Linking SysTrust to COBIT,” Volume 3, 2002, p. 45-48

“Laser Check Printing—How It Effects the Internal Control System,” Volume 4, 2002, p. 39-47

“The Global Status of Electronic Signature Legislation,” Volume 5, 2002, p. 24-26

“Auditing and Certification of a Public Key Infrastructure,” Volume 5, 2002, p. 28-31

“An Exploration of Global Perceptions of Security and Privacy,” Volume 6, 2002, p. 27-30

“The Importance of Event Correlation for Effective Security Management,” Volume 6, 2002, p. 37-38

“Application Risk in a TCP/IP Environment,” Volume 6, 2002, p. 39-40

“Web Application Security,” Volume 6, 2002, p. 44-46

“Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems,” Volume 1, 2003, p. 37-39

“Security Architecture: One Practitioner’s View,” Volume 1, 2003, p. 24-28

“The Computer Forensics and Cybersecurity Governance Model,” Volume 2, 2003, p. 41-47

“Implementing Enterprise Security: A Case Study” (Part 1), Volume 2, 2003, p. 34-39

“Implementing Enterprise Security: A Case Study” (Part 2), Volume 3, 2003, p. 60-63

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

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

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

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

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

**Note: Publications in bold are available in the ISACA Bookstore, [www.isaca.org/bookstore](http://www.isaca.org/bookstore)**

# Candidate's Guide to the CISM Exam

---

## Information Security Program Management (continued)

Project Management Institute, *A Guide to the Project Management Body of Knowledge*, USA, 2000

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

Schneier, Bruce; *Secrets & Lies: Digital Security in a Networked World*, John Wiley and Sons Inc., USA, 2000

**Senft, Sandra; Fredrick Gallegos; Carol Gonzales; Daniel P. Manson; *Information Technology Control and Audit*, 2<sup>nd</sup> Edition, Auerbach, USA, 2004**

Smith, Gordon E.; *Network Auditing: A Control Assessment Approach*, John Wiley & Sons Inc., USA, 1999

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

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

Swanson, Marianne; *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, SP800-26, August 2001

Tanenbaum, Andrew S.; *Modern Operating Systems*, 2<sup>nd</sup> Edition, Prentice Hall, USA, 2001, and India, 1995

Wack, John; Miles Tracy; Murugiah Souppaya; *Guidelines on Network Security Testing*, National Institute of Standards and Technology, SP800-42, October 2003

## Information Security Management

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

**Senft, Sandra; Frederick Gallegos; Carol Gonzales; Daniel P. Mason; *Information Technology Control and Audit*, 2<sup>nd</sup> Edition, Auerbach, USA, 2004**

## Response Management

*Information Systems Control Journal*, ISACA, USA:

**"Business Continuity: A Business Survival Strategy," Volume 1, 2002, p. 28-36**

**"Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans," Volume 1, 2002, p. 49-55**

**"Disaster Recovery: Testing an Organization's Plans," Volume 1, 2002, p. 49-55**

**"Lessons from Tragedy," Volume 1, 2002, p. 11-12**

**"Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program," Volume 3, 2002, p. 25-27**

**"The Importance of Event Correlation for Effective Security Management," Volume 6, 2002, p. 36-38**

**"Business Continuity Management Standards—A Side-by-side Comparison," Volume 2, 2003, p. 26-28**

**"The Changing Realities of Recovery: How Onsite and Mobile Options Revolutionized the Business Continuity Industry," Volume 2, 2003, p. 30-32**

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

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

**Toigo, Jon William; *Disaster Recovery Planning: Preparing for the Unthinkable*, Prentice Hall, 2002**

# Candidate's Guide to the CISM 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 CISM examination date (see page 3).

### Professional Examination Service

You are scheduled to take the ISACA Certified Information Security Manager® (CISM®) 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](mailto: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 CISM Exam

## Sample Answer Sheet (Side 1)

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

LAST NAME (Skip a space) FIRST NAME (Skip a space) Middle Initial _____															STATE CODE _____	
PROFESSIONAL EXAMINATION SERVICE New York, N.Y. EXAMINATION(S) YOU ARE TAKING															STATE _____	
CITY															STATE _____	TODAY'S DATE _____
1 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      21 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      41 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      61 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
2 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      22 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      42 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      62 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
3 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      23 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      43 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      63 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
4 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      24 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      44 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      64 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
5 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      25 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      45 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      65 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
6 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      26 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      46 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      66 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
7 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      27 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      47 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      67 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
8 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      28 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      48 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      68 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
9 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      29 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      49 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      69 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
10 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      30 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      50 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      70 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
11 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      31 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      51 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      71 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
12 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      32 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      52 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      72 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
13 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      33 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      53 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      73 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
14 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      34 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      54 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      74 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
15 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      35 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      55 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      75 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
16 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      36 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      56 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      76 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
17 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      37 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      57 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      77 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
18 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      38 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      58 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      78 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
19 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      39 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      59 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      79 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																
20 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      40 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      60 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D      80 <input type="radio"/> A <input type="radio"/> B <input type="radio"/> C <input type="radio"/> D																

PLEASE TURN OVER

# Candidate's Guide to the CISM Exam

(Side 2)

The following is a sample of a CISM 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-239649-1-554321

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  
 RIGHT     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](mailto:certification@isaca.org)

[www.isaca.org](http://www.isaca.org)