



Obtain CISM  
Certification,  
Move to  
Next Level...



## 2007 Candidate's Guide to the CISM Exam

**Exam Date: 9 June 2007**

Early Registration Deadline: 14 February 2007

Final Registration Deadline: 11 April 2007

**Exam Date: 8 December 2007**

Early Registration Deadline: 15 August 2007

Final Registration Deadline: 26 September 2007



# Candidate's Guide to the CISM Exam

---

## **ISACA®**

With more than 50,000 members in more than 140 countries, ISACA ([www.isaca.org](http://www.isaca.org)) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 50,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 6,000 professionals since its inception.

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

## **Disclosure**

Copyright © 2006 Information Systems Audit and Control Association. 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 1-933284-84-6

*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 Accredited Under ISO/IEC 17024:2003</b> . . . . .	<b>.2</b>
<b>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>.6</b>
<b>Types of Questions on the CISM Exam</b> . . . . .	<b>.7</b>
<b>Application for CISM Certification</b> . . . . .	<b>.8</b>
<b>Requirements for Initial CISM Certification</b> . . . . .	<b>.9</b>
<b>Requirements for Maintaining CISM Certification</b> . . . . .	<b>.9</b>
<b>Revocation of CISM Certification</b> . . . . .	<b>.9</b>
<b>ISACA Code of Professional Ethics</b> . . . . .	<b>.9</b>
<b>Content of the CISM Exam</b> . . . . .	<b>.10</b>
<b>Reference Materials</b> . . . . .	<b>.16</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 in 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 a CISM

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 result is 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 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 CISM Certification Board oversees the development of the exam and ensures the currency of its content. Questions for the CISM exam are developed through a comprehensive process designed to ensure the ultimate quality of the exam. The process includes a Test Enhancement Committee. Members of which work with item writers to develop and review questions before they are submitted to the CISM Certification Board for review.

The detailed job practice areas (see the Content of the CISM Exam section on page 10) 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's 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 exam consists of 200 questions and is administered biannually in June and December during a four-hour session. Candidates may take the exam in English, Japanese and Spanish.

### Exam Registration Changes

A US \$50 fee is required for all changes to the CISM exam site and/or language received between 20 April and 27 April 2007 for the June exam. **No changes will be accepted after 27 April 2007.**

A US \$50 fee is required for all changes to the CISM exam site and/or language received between 12 October and 26 October 2007 for the December exam. **No changes will be accepted after 26 October 2007.**

### 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 20 April 2007 for the June exam and 12 October 2007 for the December exam. All requests after the respective dates will be denied. **Exam registration and membership fees are nontransferable.**

**Deferral:** Candidates unable to take the exam can request a deferral of their registration fees to the next exam date. For the June 2007 exam, deferral requests received on or before 2 May 2007 will be charged a US \$50 processing fee. From 3 May 2007 through 1 June 2007, a processing fee of US \$100 will be charged. Deferral requests for the June exam will not be accepted after 1 June 2007.

For the December 2007 exam, deferral requests received on or before 31 October 2007 will be charged a US \$50 processing fee. From 1 November 2007 through 30 November 2007, a processing fee of US \$100 will be charged. Deferral requests for the December exam will not be accepted after 30 November 2007.

To request a deferral, please visit [www.isaca.org/examdefer](http://www.isaca.org/examdefer).

**The exam and deferral fees are nonrefundable. NO REFUNDS OR EXCHANGES WILL BE GIVEN FOR STUDY AIDS, ASSOCIATED TAXES, SHIPPING AND HANDLING CHARGES OR MEMBERSHIP FEES.**

# Candidate's Guide to the CISM Exam

## Study Aids for the CISM Exam

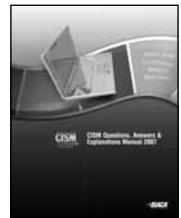
Passing the CISM exam can be achieved through an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see [www.isaca.org/cismbooks](http://www.isaca.org/cismbooks) for more details). Order early: the delivery time can be one to four weeks depending on geographic location and custom clearance practices. For current shipping information see [www.isaca.org/shipping](http://www.isaca.org/shipping).

- 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 admission ticket and exam answer sheet.
- The *CISM Review Manual 2007* is a reference guide designed to assist individuals in preparing for the CISM exam and for individuals wanting to learn more about the role and responsibilities of an information security manager. The 2007 edition has been updated to reflect the new 2007 CISM job practice and has been significantly enhanced to provide updates to the content reflecting industry changes and expanded coverage of all 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. The manual also contains applicable information security management principles, practices and strategies; detailed references where additional guidance can be found; definitions of terms; and practical examples to facilitate the learning process. 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 Questions, Answers & Explanations Manual 2007* consists of 300 multiple-choice study questions. These items appeared in the *CISM Review Questions, Answers & Explanations Manual 2006* and in the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*, but many have been enhanced or rewritten to recognize a change in practice and provide further clarity or explanation of the suggested correct answer. Some new questions have also been included that are more representative of the current exam question format. These questions are not actual exam items, but 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 exam. Questions are also sorted by CISM areas and a 200-question sample exam is provided. This publication is ideal to use in conjunction with the *CISM Review Manual 2007* and the *CISM Review Questions, Answers & Explanations Manual 2007 Supplement*.
- The *CISM Review Questions, Answers and Explanations Manual 2007 Supplement* consists of 100 multiple-choice study questions arranged in the same proportion as the most recent 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 exam and are not actual test items. This publication is ideal to use in conjunction with the *CISM Review Manual 2007* and the *CISM Review Questions, Answers & Explanations Manual 2007*.
- CISM Practice Question Database v7 combines the 400 questions, answers and explanations included in the *CISM Review Questions, Answers & Explanations Manual 2007* and the *CISM Review Questions, Answers & Explanations Manual 2007 Supplement*. The questions are sorted based on the CISM job practice areas. The new software engine can generate customized study sessions based upon previous scoring history. With this product, CISM candidates can identify strengths and weaknesses and thus focus their study efforts as needed. Students can choose various length study sessions, sample exams with randomly chosen questions and to review the results by area. Sample exams can also be chosen by area allowing for concentrated study one area at a time and by other sort features. Also included are *Information Systems Control Journal*® articles referenced in the *CISM Review Manual 2007*. Available in CD-ROM format or web site download.

PLEASE NOTE system requirements:

- Intel Pentium 3 or higher (Pentium 4 recommended)
  - Windows 98SE or higher
  - 256 MB RAM (512 MB Recommended)
  - Hard drive with up to 225MB of available space
  - CD-ROM Drive
  - Display with recommended resolution of 1024x768
- CISM 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 CISM's 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](http://www.isaca.org/chapters) and [www.isaca.org/cismcourses](http://www.isaca.org/cismcourses), respectively. A two-day review course also precedes the ISACA EuroCACS Conference, 18-21 March 2007 in Vienna, Austria, and the North America CACS Conference, 21-22 April 2007 in Grapevine (Dallas), Texas, USA.

*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.*



# Candidate's Guide to the CISM Exam

---

## 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 an e-ticket, candidates must have a current e-mail address on file. If candidate's e-mail address changes, he/she should update his/her profile on the ISACA web site ([www.isaca.org](http://www.isaca.org)) or contact [certification@isaca.org](mailto:certification@isaca.org).

**It is imperative that candidates note the specific registration and exam time on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.** Any candidate who arrives after the oral instructions begin will not be allowed to sit for the exam and will forfeit his/her registration fees. An admission ticket can only be used at the designated test center specified on the admission ticket.

If a candidate has not received either version of the admission ticket by 1 June 2007 for the June administration or by 1 December 2007 for the December administration, he/she should 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 the admission ticket at each center. All candidates must be registered and in the test center when the chief examiner begins reading the oral instructions.

### Remember to Bring 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/her registration fee.

### 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.
- No food or beverages allowed.

### 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 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.

# Candidate's Guide to the CISM 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 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 One's Time

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

## Conduct Oneself Properly

- To protect the security of the exam and maintain the validity of the scores, candidates are asked to sign the answer sheet.
- The 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 its 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 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. ISACA uses and reports scores on a common scale from 200 to 800. A scaled score of 450 or above represents a passing score for the entire exam.

**Test scores will not be available until approximately eight (8) 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. This e-mail notification will only be sent to the e-mail address listed in the candidate's profile at the time of the initial release of the results. To prevent the e-mail notification from being sent to a spam folder, candidates should add *certification@isaca.org* to their address book, whitelist or safe-senders list.**

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.

# Candidate's Guide to the CISM Exam

---

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

Candidates receiving a failing score on the exam may request a hand score of their answer sheets. This procedure ensures that no stray marks, multiple responses or other conditions interfered with computer scoring. Candidates should understand, however, that all scores are subjected to several quality control checks before they are reported; therefore, rescoring most likely will not result in a score change. Requests for hand scoring must be made in writing to the certification department within 90 days following the release of the exam results. Requests for a hand score after the deadline date will not be processed. All requests must include a candidate's name, exam identification number and mailing address. A fee of US \$50 must accompany each request.

## Types of Questions on the 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. A CISM exam question may require the candidate to choose the appropriate answer based on a qualifier, such as **MOST** likely or **BEST**. In every case, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible.

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
  
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

# Candidate's Guide to the CISM Exam

---

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 Review Questions, Answers & Explanations Manual 2007*.

## Application for CISM Certification

Passing the exam does not mean a candidate is a CISM. Once a candidate passes the CISM 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 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 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 CISM status.

## Requirements for Initial CISM Certification

Certification is granted initially 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.

### Experience Substitutions

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

Two years of the information security management work experience may be substituted with 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.

# Candidate's Guide to the CISM Exam

---

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 professional education policy requires the attainment of continuing professional education (CPE) 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 CPE hours.
- Submit annual CPE maintenance fees to ISACA International Headquarters in full.
- Attain and report a minimum of 120 CPE hours for a three-year reporting period.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with ISACA's Code of Professional Ethics.

**Failure to comply with these general requirements will result in the revocation of an individual's 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 professional education policy
- Violating any provision of the ISACA Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CISM 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 CISM Exam

---

## 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/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.

The current practice areas for the CISM exam are:

- **Information Security Governance (23%)**
- **Information Risk Management (22%)**
- **Information Security Program Development (17%)**
- **Information Security Program Management (24%)**
- **Incident Management and Response (14%)**

*Note:* The percentages listed with the job practice areas indicate the emphasis or percent of questions that will appear on the CISM exam from each area. Each practice area's definition, task and knowledge statements are included in the following table.

# Candidate's Guide to the CISM Exam

<b>CONTENT AREA</b>
<b>Information Security Governance</b>
Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.
<b>Tasks</b>
Develop an information security strategy aligned with business goals and objectives.
Align information security strategy with corporate governance.
Develop business cases justifying investment in information security.
Identify current and potential legal and regulatory requirements affecting information security.
Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
Obtain senior management commitment to information security.
Define roles and responsibilities for information security throughout the organization.
Establish internal and external reporting and communication channels that support information security.
<b>Knowledge Statements</b>
Knowledge of business goals and objectives
Knowledge of information security concepts
Knowledge of the components that comprise an information security strategy (e.g., processes, people, technologies, architectures)
Knowledge of the relationship between information security and business functions
Knowledge of the scope and charter of information security governance
Knowledge of the concepts of corporate and information security governance
Knowledge of methods of integrating information security governance into the overall enterprise governance framework
Knowledge of budgetary planning strategies and reporting methods
Knowledge of business case development
Knowledge of the types and impact of internal and external drivers (e.g., technology, business environment, risk tolerance) that may affect organizations and information security
Knowledge of regulatory requirements and their potential business impact from an information security standpoint
Knowledge of common liability management strategies and insurance options (e.g., crime or fidelity insurance, business interruptions)
Knowledge of third-party relationships and their impact on information security (e.g., in cases of mergers and acquisitions)
Knowledge of methods used to obtain senior management commitment to information security
Knowledge of the establishment and operation of an information security steering group
Knowledge of information security management roles, responsibilities and general organizational structures
Knowledge of approaches for linking policies to enterprise business objectives
Knowledge of generally accepted international standards for information security management
Knowledge of centralized and distributed methods of coordinating information security activities
Knowledge of methods for establishing reporting and communication channels throughout an organization
<b>Information Risk Management</b>
Identify and manage information security risks to achieve business objectives.
<b>Tasks</b>
Establish a process for information asset classification and ownership.
Implement a systematic and structured information risk assessment process.
Ensure that business impact assessments are conducted periodically.
Ensure that threat and vulnerability evaluations are performed on an ongoing basis.

# Candidate's Guide to the CISM Exam

<b>CONTENT AREA</b>
<b>Information Risk Management (continued)</b>
Identify and periodically evaluate information security controls and countermeasures to mitigate risks to acceptable levels.
Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., development, procurement and employment life cycles).
Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.
<b>Knowledge Statements</b>
Knowledge of required components for establishing an information classification schema consistent with business objectives (including the identification of assets)
Knowledge of the components of information ownership schema (including drivers of the schema such as roles and responsibilities)
Knowledge of information threats, vulnerabilities and exposures
Knowledge of information resource valuation methodologies
Knowledge of risk assessment and analysis methodologies (including measurability, repeatability and documentation)
Knowledge of factors used to determine risk reporting frequency and requirements
Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events on the business
Knowledge of baseline modeling and its relationship to risk-based assessments of control requirements
Knowledge of information security controls and countermeasures
Knowledge of methods of analyzing effectiveness of information security controls and countermeasures
Knowledge of risk mitigation strategies used in defining security requirements for information resources
Knowledge of gap analysis to assess generally accepted standards of good practice for information security management against the current state
Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks to acceptable levels
Knowledge of life cycle-based risk management principles and practices
<b>Information Security Program Development</b>
Create and maintain a program to implement the information security strategy.
<b>Tasks</b>
Develop and maintain plans to implement the information security strategy.
Specify the activities to be performed within the information security program.
Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).
Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
Ensure the development of information security architectures (e.g., people, processes, technology).
Establish, communicate and maintain information security policies that support the security strategy.
Design and develop a program for information security awareness, training and education.
Ensure the development, communication and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
Establish metrics to evaluate the effectiveness of the information security program.

# Candidate's Guide to the CISM Exam

<b>CONTENT AREA</b>
<b>Information Security Program Development (continued)</b>
<i>Knowledge Statements</i>
Knowledge of methods to interpret strategies into manageable and maintainable plans for implementing information security
Knowledge of the types of activities required within an information security program
Knowledge of methods for managing the implementation of the information security program
Knowledge of planning, designing, developing, testing and implementing information security controls
Knowledge of methods to align information security program requirements with those of other assurance functions (e.g., physical, HR, quality, IT)
Knowledge of how to identify internal and external resources and skills requirements (e.g., finances, people, equipment, systems)
Knowledge of resources and skills acquisition (e.g., project budgeting, employment of contract staff, equipment purchase)
Knowledge of information security architectures (e.g., logical architectures and physical architectures) and their deployment
Knowledge of security technologies and controls (e.g., cryptographic techniques, access controls, monitoring tools)
Knowledge of the process for developing information security policies that meet and support enterprise business objectives
Knowledge of content for information security awareness, training and education across the enterprise (e.g., general security awareness, writing secure code, operating security controls)
Knowledge of methods to identify activities to close the gap between proficiency levels and skill requirements
Knowledge of activities to foster a positive security culture and behavior
Knowledge of the uses of and differences between policies, standards, procedures, guidelines and other documentation
Knowledge of process for linking policies to enterprise business objectives
Knowledge of methods to develop, implement, communicate and maintain information security policies, standards, procedures, guidelines and other documentation
Knowledge of methods of integrating information security requirements into organizational processes (e.g., change control, mergers and acquisitions)
Knowledge of life cycle methodologies and activities (e.g., development, employment, procurement)
Knowledge of processes for incorporating security requirements into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties)
Knowledge of methods and techniques to manage third-party risks (e.g., service level agreements, contracts, due diligence, suppliers, subcontractors)
Knowledge of the design, development and implementation of information security metrics
Knowledge of certifying and accrediting the compliance of business applications and infrastructures to business needs
Knowledge of methods for ongoing evaluation of the effectiveness and applicability of information security controls (e.g., vulnerability testing, assessment tools)
Knowledge of methods of tracking and measuring the effectiveness and currency of information security awareness, training and education
Knowledge of methods of sustaining the information security program (e.g., succession planning, allocation of jobs, documentation of the program)
<b>Information Security Program Management</b>
Oversee and direct information security activities to execute the information security program.
<i>Tasks</i>
Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed.
Ensure that information security is an integral part of the systems development process.

# Candidate's Guide to the CISM Exam

<b>CONTENT AREA</b>
<b>Information Security Program Management (<i>continued</i>)</b>
Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.
Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).
Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
Ensure that noncompliance issues and other variances are resolved in a timely manner.
<b><i>Knowledge Statements</i></b>
Knowledge of how to interpret information security policies and implement them
Knowledge of information security administrative processes and procedures (e.g., access controls, identity management, remote access)
Knowledge of methods for managing the enterprise's information security program through third parties (e.g., trade partners, contractors, joint ventures, outsourcing providers)
Knowledge of methods for managing the enterprise's information security program through security services providers
Knowledge of information security-related contract provisions (e.g., right to audit, confidentiality, nondisclosure)
Knowledge of methods to define and monitor security requirements in service level agreements (SLAs)
Knowledge of methods and approaches to providing continuous monitoring of security activities in the enterprise's infrastructure and business applications
Knowledge of management metrics to validate the information security program investment (e.g., data collection, periodic review, key performance indicators)
Knowledge of methods of testing the effectiveness and applicability of information security controls (e.g. penetration testing, password cracking, social engineering, assessment tools)
Knowledge of change and configuration management activities
Knowledge of the advantages/disadvantages of using internal/external assurance providers to perform information security reviews
Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information
Knowledge of external vulnerability reporting sources for information on potential impacts on information security in applications and infrastructure
Knowledge of events affecting security baselines that may require risk reassessments and changes to information security program elements
Knowledge of information security problem management practices
Knowledge of reporting requirements of systems and infrastructure security status
Knowledge of general line-management techniques including budgeting (e.g., estimating, quantifying, trade-offs), staff management (e.g., motivating, appraising, objective-setting) and facilities (e.g., obtaining and using equipment)
<b>Incident Management and Response</b>
Plan, develop and manage a capability to detect, respond to and recover from information security incidents.
<b><i>Tasks</i></b>
Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.
Establish escalation and communication processes and lines of authority.
Develop plans to respond to and document information security incidents.
Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).

# Candidate's Guide to the CISM Exam

<b>CONTENT AREA</b>
<b>Incident Management and Response (<i>continued</i>)</b>
Integrate information security incident response plans with the organization's disaster recovery plan (DRP) and business continuity plan (BCP).
Organize, train and equip teams to respond to information security incidents.
Periodically test and refine information security incident response plans.
Manage the response to information security incidents.
Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.
<b><i>Knowledge Statements</i></b>
Knowledge of the components of an incident response capability
Knowledge of recovery planning and business continuity planning
Knowledge of information incident management practices
Knowledge of disaster recovery testing for infrastructure and critical business applications
Knowledge of events that trigger incident response
Knowledge of methods of containing damage
Knowledge of notification and escalation processes for effective security management
Knowledge of the role of individuals in identifying and managing security incidents
Knowledge of crisis communications
Knowledge of methods identifying business resources essential to recovery
Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams
Knowledge of forensic requirements for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)
Knowledge used to document incidents and subsequent actions
Knowledge of internal and external reporting requirements
Knowledge of postincident review practices and investigative methods to identify causes and determine corrective actions
Knowledge of techniques for quantifying damages, costs and other business impacts arising from security incidents
Knowledge of recovery time objective (RTO) and its relationship to business continuity planning objectives and processes

# Candidate's Guide to the CISM Exam

---

The following are references recommended for further study in preparation for the exam. A more comprehensive list can be found in the *CISM Review Manual 2007*.

## Chapter 1 Reference Materials

Andrews, Kenneth; *The Concept of Corporate Strategy, 2<sup>nd</sup> Edition*, Dow-Jones Irwin, 1994

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

Business Roundtable, "Building Security in the Digital Resource: An Executive Resource," November 2002, [www.businessroundtable.org](http://www.businessroundtable.org)

Business Roundtable, "Information Security Addendum to Principles of Corporate Governance," April 2003, [www.businessroundtable.org](http://www.businessroundtable.org)

Carnegie Mellon University, *Governing for Enterprise Security*, USA, June 2005

The Information Security Forum, *The Standard of Good Practice for Information Security*, January 2005, [www.isfsecuritystandard.com/index\\_ie.htm](http://www.isfsecuritystandard.com/index_ie.htm)

Information Systems Security Association (ISSA), *The Generally Accepted Information Security Principles (GAISP)*, May 2005

The Institute of Internal Auditors (IIA), *Presenting the Information Security Case to the Board of Directors*, 2001

**IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2005, 2000, 1996, [www.isaca.org/cobit](http://www.isaca.org/cobit)**

**IT Governance Institute, *IT Governance Domain Practices and Competencies series*, USA, 2005**

Kiely, Laree; Terry Benzel; *Systemic Security Management*, Libertas Press, 2006

Organisation for Economic Co-operation and Development, "OECD Principles of Corporate Governance," 1999, 2004, [www.oecd.org/document/49/0,2340,en\\_2649\\_34813\\_31530865\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/49/0,2340,en_2649_34813_31530865_1_1_1_1,00.html)

Organization for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, France, 2002

**Sherwood, John; Andrew Clark; David Lynas; *Enterprise Security Architecture: A Business Driven Approach*, CMP, 2005**

## Chapter 2 Reference Materials

**Hardy, Gary; Lighthouse Global; *Information Risks: Whose Business Are They?*, IT Governance Institute, USA, 2005**

**IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2005, 2000, 1996, [www.isaca.org/cobit.htm](http://www.isaca.org/cobit.htm)**

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

**Sherwood, J.; A. Clark; D. Lynas; *Enterprise Security Architecture: A Business Driven Approach*, CMP Books, 2005**

**Van Grembergen, Wim; Steven De Haes; *Measuring and Demonstrating the Value of IT*, IT Governance Institute, USA, 2005**

## Chapter 3 Reference Materials

Axelrod, C. Warren; *Outsourcing Information Security*, Artech House, 2004

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

Information Security Forum, *The Standard of Good Practice for Information Security*, January 2005, [www.isfsecuritystandard.com](http://www.isfsecuritystandard.com)

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

---

International Organisation for Standardisation (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

**IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2005, 2000, 1996, [www.isaca.org/cobit](http://www.isaca.org/cobit)**

Kiely, Laree; Terry Benzel; *Systemic Security Management*, USC Marshall School of Business, Institute for Critical Information Infrastructure Protection, 2006

Kovacich, Gerald; *The Information Systems Security Officer's Guide, 2<sup>nd</sup> Edition*, Butterworth-Heinemann, an imprint of Elsevier Science, 2003

National Institute of Standards and Technology, "Security Metrics Guide for Information Technology Systems," NIST Special Publication 800-55, USA, July 2003

Paulk, Mark, et.al; Carnegie Mellon University, Software Engineering Institute, *The Capability Maturity Model*, Addison-Wesley, 1995

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

## Chapter 4 Reference Materials

German Federal Office for Information Security, *IT Baseline Protection Manual*, Germany, 2004, [www.bsi.bund.de/english/gshb/index.htm](http://www.bsi.bund.de/english/gshb/index.htm)

International System Security Engineering Association (ISSEA), "System Security Engineering Capability Maturity Model," [www.issea.org/sse\\_cmm/sse\\_cmm.html](http://www.issea.org/sse_cmm/sse_cmm.html)

**IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2005, 2000, 1996, [www.isaca.org/cobit](http://www.isaca.org/cobit)**

Krause, Micki; Harold Tipton; *Handbook of Information Security Management, 4<sup>th</sup> Edition*, Auerbach Publications, 2004

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

**Van Grembergen, Wim; Steven De Haes; *Measuring and Demonstrating the Value of IT*, IT Governance Institute, USA, 2005**

**Wulgaert, Tim; *Security Awareness: Best Practices to Secure Your Enterprise*, ISACA, USA, 2005**

## Chapter 5 Reference Materials

**Endorf, Carl; Eugene Schultz; Jim Mellander; *Intrusion Detection and Prevention*, McGraw-Hill, USA, 2004**

Fraser, B. (Ed.); *Site Security Handbook*, RFC 2196, 1997, [www.ietf.org](http://www.ietf.org)

Grance, T.; K. Kent; B. Kim; *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Publication 800-61, 2003, <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Mandia, K.; C. Prosis; M. Pepe; *Incident Response and Computer Forensics, 2<sup>nd</sup> Edition*, McGraw-Hill, USA, 2003

Northcutt, S.; *Network Intrusion Detection: An Analyst's Handbook*, New Riders, USA, 2002

Schultz, E.E.; R.M. Shumway; *Incident Response: A Strategic Guide for Handling Security Incidents in Systems and Networks*, New Riders, USA, 2001

Schultz, E. E.; E. Spafford; *Intrusion Detection: How to Utilize a Still Immature Technology*, In Tipton, H. and Krause, M., *Information Security Management Handbook, 4<sup>th</sup> Edition*, USA, Auerbach, 2000

# Candidate's Guide to the CISM Exam

---

## Sample Admission Ticket

The following is an example of the admission ticket that candidates will receive approximately two to three weeks prior to the CISM exam date (see page 4).

---

**PES (on behalf of ISACA)  
475 Riverside Drive, New York, NY 10115**

You are scheduled to take the ISACA Certified Information Security Manager® (CISM®) Exam on **Saturday, 9 June 2007**. Report no later than **XX:XX AM** on the morning of the exam to the test site listed below. The Chief Examiner will begin reading the instructions at **XX:XX AM**.

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

The timed portion of the exam is four (4) hours from **XX:XX AM** to **XX:XX PM**. The beginning time may vary slightly due to the registration process.

TEST CENTER (Code #XXXX )  
Test Center Name  
Street Address  
City, State, Postal Code or Zip Code  
Country  
Website or Directions if available

Your Identification Number is (ID# XXXXXXXXX )

You are scheduled for the **XXXXXXX** language version of the exam.

YOU MUST bring this admission ticket, several sharpened No.2 or HB pencils, an eraser, and an original acceptable form of identification with a photo, 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 and take the exam and will forfeit their registration fee. Candidates are not allowed to bring in any types of communication device, i.e., cell phones, PDA's, BlackBerries. Please retain this admission ticket for future reference.

If you have any questions, please contact ISACA at +1.847.253.1545, ext. 403, 471 or 474, or via e-mail at [certification@isaca.org](mailto:certification@isaca.org).

---

### ISACA

Test date: Saturday, 9 June 2007: **XXXX**

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#: XXXXXXXXX

Name

Address 1

Address 2

Address 3

Address 4

Address 5



# Candidate's Guide to the CISM Exam

(Side 2)

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 Reflector 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

WRONG       RIGHT

WRONG       RIGHT



**3701 Algonquin Road, Suite 1010**

**Rolling Meadows, IL 60008 USA**

**Phone: +1.847.253.1545**

**Fax: +1.847.253.1443**

**E-mail: *certification@isaca.org***

**Web site: *www.isaca.org***