



**Candidate's Guide to the  
CISM<sup>®</sup> Exam and Certification**

# Candidate's Guide to the CISM Exam and Certification

---

## **ISACA®**

With more than 65,000 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. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 50,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by 7,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

## **Disclaimer**

ISACA and the 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 © 2007 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: [examregistrant@isaca.org](mailto:examregistrant@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

ISBN 978-1-60420-063-8

*Candidate's Guide to the CISM Exam*

Printed in the United States of America

## Table of Contents

|  |            |
|--|------------|
| <b>Introduction</b> .....  | <b>.2</b>  |
| <b>CISM Program Accreditation Renewed<br/>Under ISO/IEC 17024:2003</b> ..... | <b>.2</b>  |
| <b>The CISM Exam</b> .....   | <b>.2</b>  |
| <b>Content of the CISM Exam</b> .....  | <b>.3</b>  |
| <b>Study Aids for the CISM Exam</b> .....                                    | <b>.3</b>  |
| <b>Administration of the CISM Exam</b> .....                                 | <b>.3</b>  |
| <b>Scoring the CISM Exam</b> .....   | <b>.5</b>  |
| <b>Types of Questions on the CISM Exam</b> .....                             | <b>.5</b>  |
| <b>Application for CISM Certification</b> .....                              | <b>.6</b>  |
| <b>Requirements for Initial CISM Certification</b> .....                     | <b>.7</b>  |
| <b>Requirements for Maintaining CISM Certification</b> .....                 | <b>.7</b>  |
| <b>Revocation of CISM Certification</b> .....                                | <b>.8</b>  |
| <b>ISACA Code of Professional Ethics</b> .....                               | <b>.8</b>  |
| <b>CISM Task and Knowledge Statements</b> .....                              | <b>.9</b>  |
| <b>Suggested Resources for Further Study</b> .....                           | <b>.14</b> |
| <b>Sample Admission Ticket</b> .....   | <b>.17</b> |
| <b>Sample Answer Sheet</b> .....   | <b>.19</b> |

# Candidate's Guide to the CISM Exam and Certification

---

## 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.

## CISM Program Accreditation Renewed 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's will continue to present themselves around the world.

## 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 content areas 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. For a current list of languages, please visit [www.isaca.org/cismterminology](http://www.isaca.org/cismterminology).

# Candidate's Guide to the CISM Exam and Certification

---

## 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 table on page 9.

## Study Aids for the CISM Exam

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

*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 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 [examregistrant@isaca.org](mailto:examregistrant@isaca.org).

**It is imperative that candidates note the specific registration and exam time on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.** Any candidate who arrives after the oral instructions 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.

### Be Prompt

Registration will begin at the time indicated on the admission ticket at each center. All candidates must be registered and in the test center when the chief examiner begins reading the oral instructions. **NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS.**

# Candidate's Guide to the CISM Exam and Certification

---

## Remember to Bring the Admission Ticket

Candidates can use their admission ticket only at the designated test center. Only those candidates with a **valid admission ticket and an acceptable form of original identification** will be admitted. Candidates will be admitted to the test center only if they have a valid admission ticket and an acceptable form of identification (ID). An acceptable form of ID must be a current and original government issued identification that contains the candidate's name, as it appears on the admission ticket, and the candidate's photograph. All of these characteristics must be demonstrated by the single piece of ID provided. Examples include, but are not limited to a passport, driver's license, military ID, date ID, greencard and national ID. 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.

The complete Personal Belongings Policy is available at [www.isaca.org/cismbelongings](http://www.isaca.org/cismbelongings).

## 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.
- 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.

# Candidate's Guide to the CISM Exam and Certification

---

## Reasons for Dismissal

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

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

## Scoring the 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 *examregistrant@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.

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.

# Candidate's Guide to the CISM Exam and Certification

---

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. The option in bold is the correct answer.

1. Which of the following is **MOST** indicative of the failure of information security governance within an organization?

- A. The information security department has had difficulty filling vacancies.
- B. The chief information officer (CIO) approves changes to the security policy.
- C. The information security oversight committee only meets quarterly.
- D. The data center manager has final sign-off on all security projects.**

2. Which of the following would be the **MOST** appropriate task for a chief information security officer to perform?

- A. Update platform-level security settings.
- B. Conduct disaster recovery test exercises.
- C. Approve access to critical financial systems.
- D. Develop an information security strategy paper.**

3. A risk assessment should be conducted:

- A. once for each business process and subprocess.
- B. every three to five years for critical business processes.
- C. by external parties to maintain objectivity.
- D. annually or whenever there is a significant change.**

4. Which of the following **BEST** indicates the probability that a successful attack will occur?

- A. Value of the target and level of protection is high.
- B. Motivation and ability of the attacker is high.
- C. Value of the target is high and protection is low.**
- D. Motivation of the attacker and value of the target is high.

5. An information security program should be sponsored by:

- A. infrastructure management.
- B. the corporate legal department.
- C. key business process owners.**
- D. quality assurance management.

## 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.

# Candidate's Guide to the CISM Exam and Certification

---

## 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.

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

CISMs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 CPE hours. The CISM continuing professional education policy requires the attainment of continuing professional education (CPE) hours over an annual and three-year reporting period.
- Attain and report a minimum of 120 CPE hours for a three-year reporting period.
- Submit annual CPE maintenance fees to ISACA International Headquarters in full.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with ISACA's Code of Professional Ethics.

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

# Candidate's Guide to the CISM Exam and Certification

---

## 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 and Certification

## CISM Task and Knowledge Statements

| <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 and Certification

| <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 and Certification

| <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 and Certification

| <b>CONTENT AREA</b>  |
|--|
| <b>Information Security Program Management (continued)</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>Knowledge Statements</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>Tasks</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 and Certification

| <b>CONTENT AREA</b>   |
|---|
| <b>Incident Management and Response (continued)</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>Knowledge Statements</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 and Certification

---

## Suggested Resources for Further Study

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

### Content Area 1—Information Security Governance

Aberdeen Group, "Best Practices in Security Governance," Aberdeen Group, USA, 2005

Allen, Julia; *Governing for Enterprise Security*, Carnegie Mellon University, USA, 2005

Australian Computer Emergency Response Team, [www.auscert.org.au](http://www.auscert.org.au)

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

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

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)

International Organization for Standardization (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, 2007, 2005, 2000, 1996, [www.isaca.org/cobit](http://www.isaca.org/cobit)**

**IT Governance Institute, *Board Briefing on IT Governance, 2<sup>nd</sup> Edition*, USA, 2003**

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

McKinsey and Institutional Investors Inc., "McKinsey/KIOD Survey on Corporate Governance," January 2003

Meta Group, *Plan for a Security Architecture Guidelines and Relationships*, 2002

National Cyber Security Partnership, [www.cyberpartnership.org/init-governance.html](http://www.cyberpartnership.org/init-governance.html)

National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems*, NIST 800-53, USA, 2005

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

**Pironti, John P.; "Information Security Governance: Motivations, Benefits and Outcomes," *Information Systems Control Journal*, vol. 4, 2006, p. 45**

PricewaterhouseCoopers, *The Global State of Information Security*, 2005

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

### Content Area 2—Information Risk Management

Australian Standard; AS/NZS 4360, Risk Management, [www.riskmanagement.com.au](http://www.riskmanagement.com.au)

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

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

# Candidate's Guide to the CISM Exam and Certification

---

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

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

IT Governance Institute, *IT Governance Implementation Guide: Using COBIT® and Val IT™*, 2<sup>nd</sup> Edition, USA, 2007

National Institute of Standards and Technology (NIST), *Risk Management Guide for Information Technology Systems*, USA, SP 80030, 2002

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

Survive, [www.survive.com](http://www.survive.com)

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

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

## Content Area 3—Information Security Program Development

Allen, Julia; *The CERT Guide to System and Network Security Practices*, Addison-Wesley, USA, 2001

Amoroso, Ed; *Intrusion Detection*, Intrusion.net Books, USA, 1999

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

Hardy, Gary; Lighthouse Global; *IT Governance Domain Practices and Competencies Series*, IT Governance Institute, USA, 2005

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

IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2007, 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, USA, 2006

Project Management Institute Inc., *A Guide to the Project Management Body of Knowledge (PMBOK Guide), Third Edition*, USA, 2004

SANS Institute, *The SANS Security Policy Project*, [www.sans.org](http://www.sans.org)

Sherwood, J.; A. Clark; D. Lynas; *Enterprise Security Architecture: A Business Driven Approach*, CMP Books, USA, 2005, [www.sabsa.org](http://www.sabsa.org)

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

Viega, John; Gary McGraw; *Building Secure Software*, Addison-Wesley, USA, 2002

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

# Candidate's Guide to the CISM Exam and Certification

---

## Content Area 4—Information Security Program Management

Bonham, Stephen S.; *IT Project Portfolio Management*, Artech House, USA, 2005

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

International Federation of Accountants (IFAC), "Managing Security of Information Guidelines," 2006, [www.ifac.org](http://www.ifac.org)

International Organization for Standardization (ISO), "Guidelines for the Management of IT Security," ISO/IEC 13335, 2006, [www.iso.org](http://www.iso.org)

IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, USA, 2007, 2005, 2000, 1996, [www.isaca.org/cobit](http://www.isaca.org/cobit)

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

## Content Area 5—Incident Management and Response

Alberts, Chris; Audrey Dorofee; Georgia Killcrece; Robin Ruefle; Mark Zajicek; "Defining Incident Management Processes for CSIRTs: A Work in Progress"; Software Engineering Institute, Carnegie Mellon University, USA, 2007, [www.sei.cmu.edu/publications/documents/04.reports/04tr015.html](http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html)

Carnegie Mellon University/Software Engineering Institute CERT® Coordination Center; "Creating a Computer Security Incident Response Team: A Process for Getting Started," February 2006, [www.cert.org/csirt/Creating-A-CSIRT.html](http://www.cert.org/csirt/Creating-A-CSIRT.html)

Deloitte & Touche and Information Systems Audit and Control Foundation, *e-Commerce Security—Business Continuity Planning*, USA, 2002

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

Federal Computer Incident Response Center, USA, [www.fedcirc.gov](http://www.fedcirc.gov)

Federal Emergency Management Agency, USA, [www.fema.org](http://www.fema.org)

Federal Emergency Management Agency, USA, *Global Emergency Management System*, [www.fema.gov/gems/index.jsp](http://www.fema.gov/gems/index.jsp)

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>

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

Symantec, "Managing Security Incidents in the Enterprise," [www.symantec.com/avcenter/reference/incident.manager.pdf](http://www.symantec.com/avcenter/reference/incident.manager.pdf)

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

# Candidate's Guide to the CISM Exam and Certification

## Sample Admission Ticket

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

### CISM EXAM ADMISSION TICKET

[Date]

[Exam Registrant Address]

[Exam Registrant Name]:

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

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

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

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

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

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

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

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

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

**Page intentionally left blank**



# Candidate's Guide to the CISM Exam and Certification

(Side 2)

YOUR SIGNATURE/SEAL REQUIRED HERE:

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

Mark-Rollco® by MCS EM-238649-1-554321

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***

ISBN 978-1-60420-063-8



9 0000

9 781604 200638