



CERTIFIED INFORMATION SECURITY MANAGER®

2011 Candidate's Guide to the
CISM® Exam and Certification

CISM

Candidate's Guide to the CISM® Exam and Certification

CISM Exams 2011— Important Date Information

Exam Date—11 June 2011

Early registration deadline:	9 February 2011
Final registration deadline:	6 April 2011
Exam registration changes:	Between 16 April and 22 April, charged a US \$50 fee, with no changes accepted after 22 April 2011
Refunds:	By 15 April 2011, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 22 April 2011, charged a US \$50 processing fee. Requests received from 23 April through 26 May 2011, charged a US \$100 processing fee. After 26 May 2011, no deferrals will be permitted.

Exam Date—10 December 2011

Early registration deadline:	17 August 2011
Final registration deadline:	5 October 2011
Exam registration changes:	Between 8 October and 14 October, charged a US \$50 fee, with no changes accepted after 14 October 2011
Refunds:	By 7 October 2011, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 14 October 2011, charged a US \$50 processing fee. Requests received from 15 October through 23 November 2011, charged a US \$100 processing fee. After 23 November 2011, no deferrals will be permitted.

All deadlines are based upon Chicago, Illinois, USA 5 p.m. CT (central time)

ISBN 978-1-60420-158-1
2011 *Candidate's Guide to the CISM® Exam and Certification*
Printed in the United States of America

Table of Contents

Introduction	3
CISM Program Accreditation Renewed Under ISO/IEC 17024:2003	3
The CISM Exam.....	3
Preparing for the CISM Exam.....	3
Administration of the CISM Exam.....	4
Scoring the CISM Exam.....	5
Types of Questions on the CISM Exam.....	6
Application for CISM Certification	6
Requirements for Initial CISM Certification	6
Requirements for Maintaining CISM Certification	7
ISACA Code of Professional Ethics	7
Revocation of CISM Certification.....	7
CISM Task and Knowledge Statements	8

ISACA®

With 95,000 constituents in 160 countries, ISACA® (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®) designation, earned by more than 70,000 since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 14,000 professionals since 2002; the Certified in the Governance of Enterprise IT® (CGEIT®) designation, earned by more than 4,000 professionals since 2008; and the Certified in Risk and Information Systems Control™ (CRISC™) designation.

Disclaimer

ISACA and the CISM Certification Committee have designed the *2011 Candidate's Guide to the CISM® Exam and Certification* 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.

Reservation of Rights

Copyright © 2010 ISACA. Reproduction or storage in any form for any purpose is not permitted without ISACA's prior written permission. No other right or permission is granted with respect to this work. All rights reserved.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: exam@isaca.org
Web site: www.isaca.org

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.

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 Committee 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 Subcommittee (TES) that works with item writers to develop and review questions before they are submitted to the CISM Certification Committee for review.

A job practice serves as the basis for the exam and the experience requirements to earn the CISM certification. This job practice is periodically updated and consists of five content areas (domains). The domains and the accompanying tasks and knowledge statements were the result of extensive research and feedback from subject matter experts around the world.

The tasks and knowledge statements depict the tasks performed by CISM's and the knowledge required to perform these tasks. Exam candidates will be tested based on their practical knowledge associated with performing these tasks.

The current job practice analysis contains the following domains and percentages:

- **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 domains indicate the emphasis or percentage of questions that will appear on the exam from each domain. For a description of each domain's task and knowledge statements, please refer to pages 8-11.

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

Preparing 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/cismguide to view the ISACA study aids that can help you prepare for the exam. Order early as delivery time can be from one to four weeks depending on geographic location and customs clearance practices. For current shipping information see www.isaca.org/shipping.

A comprehensive list of references recommended for study in preparation for the exam can be found in the *CISM Review Manual 2011*.

Candidate's Guide to the CISM® Exam and Certification

ISACA maintains a glossary of terms as well as glossaries specific to each certification. These glossaries are available at www.isaca.org/glossary.

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

Administration of the CISM Exam

ISACA utilizes an internationally recognized professional testing agency to assist in the construction, administration and scoring of the CISM exam.

Candidates wishing to comment on the test administration conditions may do so at the conclusion of the testing session by completing the "Test Administration Questionnaire." The Test Administration Questionnaire is presented at the back of the examination booklet and your questionnaire answers should be entered in boxes P through S of the Special Codes section (Grid No. 4) on the front of your Answer Sheet.

Candidates who wish to address any additional comments or concerns about the examination administration, including site conditions and the exam itself, should contact ISACA international head-quarters by letter or by e-mail (exam@isaca.org). These comments or concerns are to be received by ISACA within 2 weeks after the examination date. Please include the following information in your comments: exam ID number, testing site, date tested and any relevant details on the specific issue.

Alternatively, candidates who wish to comment on the contents of the examination may do so by mailing their comments to Professional Examination Service. However, only those comments received by Professional Examination Service during the first 2 weeks after the exam administration will be considered in the final scoring process of the examination. You may obtain the address of Professional Examination Service from the Proctor after you complete the examination.

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 that candidates must bring with them to take the CISM exam. With the exception of contact information changes, candidates are not to write on the admission ticket.

Please Note: In order to receive an admission ticket, all fees must be paid. Admission tickets are sent via hard copy and e-mail to the current postal mailing and e-mail address on file. Only candidates with an admission ticket and an acceptable government-issued ID will be admitted to take the exam, and the name on the admission ticket must match the name on the government-issued ID. The hard copy admission ticket or print out of the e-ticket is valid for admission into the exam. If candidates' mailing and/or e-mail addresses change, they should update their profile on the ISACA web site (www.isaca.org) or contact exam@isaca.org.

It is imperative that candidates note the specific registration and exam times on their admission ticket. NO CANDIDATE WILL BE ADMITTED TO THE TEST CENTER ONCE THE CHIEF EXAMINER BEGINS READING THE ORAL INSTRUCTIONS, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.

Any candidate who arrives after the oral instructions have begun will not be allowed to sit for the exam and will forfeit his/her registration fee. An admission ticket can only be used at the designated test center specified on the admission ticket. IDs will be checked during the exam administration.

Special Arrangements

Upon request, ISACA will make reasonable accommodations in its exam procedures for candidates with documented disabilities or religious requirements. These candidates may request consideration for reasonable alterations in exam format, presentations, food or drink at the exam site, or scheduling. Requests for food or drink at the exam site must be accompanied by a doctor's note; otherwise, **no food or drinks are allowed at any exam site**. Requests for consideration must be submitted to ISACA International Headquarters in writing, accompanied by appropriate documentation, no later than 6 April 2011 for the June 2011 exam and 5 October 2011 for the December 2011 exam.

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 room 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, APPROXIMATELY 30 MINUTES BEFORE THE EXAM BEGINS.**

Remember to Bring the Admission Ticket

Candidates can use their admission ticket (either their e-ticket or physical admission ticket) only at the designated test center. 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 ID that contains the candidate's name, as it appears on the admission ticket, and the candidate's photograph. The information on the ID cannot be handwritten. All of these characteristics must be demonstrated by the single piece of ID provided. Examples include, but are not limited to, a passport, driver's license, military ID, state ID, green card and national ID. Any candidate who does not provide an acceptable form of ID 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 center after the oral instructions have begun.
- Candidates should bring several sharpened No. 2 or HB (soft lead) pencils and a good eraser. Pencils and erasers will not be available at the test center.
- Candidates are not allowed to bring reference materials, blank paper, note pads or language dictionaries into the test center.
- Candidates are not allowed to bring or use a calculator in the test center.

Candidate's Guide to the CISM® Exam and Certification

- Candidates are not allowed to bring any type of communication device (i.e., cell phones, PDAs, Blackberries) into the test center. **If exam candidates are viewed with any such device during the exam administration, their exams will be voided and they will be asked to immediately leave the exam site.**
- Visitors are not permitted in the test center.
- No food or beverages are allowed in the test center (without advanced authorization from ISACA).

Misconduct

Candidates who are 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; using any type of communication device, including cell phones, during the exam administration; or removing the exam booklet, answer sheet or notes from the testing room—will be disqualified and may face legal action. Candidates who leave the testing area without authorization or accompaniment by a test proctor will not be allowed to return to the testing room and will be subject to disqualification. The testing agency will report such irregularities to ISACA's CISM Certification Committee.

The complete Personal Belongings Policy is available at www.isaca.org/cismbelongings. Neither ISACA nor its testing vendor takes responsibility for the personal belongings of candidates.

Be Careful in Completing the Answer Sheet

- 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 incorrectly reported.
- A proctor speaking the primary language used at each test center is available. If a candidate desires to take the exam in a language other than the primary language of the test center, 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 erase the wrong answer fully before marking in the new one.
- All questions should be answered. **There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly, so do not leave any questions blank.**
- After completion, candidates are required to hand in their answer sheet and test booklet.

Budget One's Time

- The exam, which is four hours in length, allows for a little over one minute per question. Candidates are advised to 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 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 Committee reserves the right to disqualify any candidate who is discovered engaging in any kind of misconduct or violation of exam rules, 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 center. The testing agency will provide the CISM Certification Committee with records regarding such irregularities for its review and to render a decision.

Reasons for Dismissal or Disqualification

- Unauthorized admission to the test center.
- Candidate creates a disturbance or gives or receives help.
- Candidate attempts to remove test materials or notes from the test center.
- Candidate impersonates another candidate.
- Candidate brings items into the test center that are not permitted.
- Candidate possession of any communication device (i.e., cell phone, PDA, BlackBerry®) during the exam administration
- Candidate unauthorized leave of the test area

If candidates are observed with any communication device (i.e., cell phone, PDA, BlackBerry) during the exam administration, their exams will be voided and they will be asked to immediately leave the test site.

Scoring the CISM Exam

The CISM exam consists of 200 multiple-choice items. Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. A candidate must receive a score of 450 or higher to pass the exam. For example, the scaled score of 800 represents a perfect score with all questions answered correctly; a scaled score of 200 is the lowest score possible and signifies that only a small number of questions were answered correctly. A score of 450 represents a minimum consistent standard of knowledge as established by the CISM Certification Committee. A candidate receiving a passing score may then apply for certification if all other requirements are met.

Candidate's Guide to the CISM® Exam and Certification

The CISM exam contains some questions which are included for research and analysis purposes only. These questions are not separately identified and not used to calculate your final score.

Approximately eight weeks after the test date, the official exam results will be mailed to candidates. Additionally, with the candidate's consent on the registration form, an e-mail message containing the candidate's pass/fail status and score will be sent to the candidate. This e-mail notification will only be sent to the address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax. To prevent e-mail notification from being sent to spam folders, candidates should add *exam@isaca.org* to their address book, whitelist or safe-senders list.

Candidates will receive a score report containing a subscore for each domain area. Successful candidates will receive, along with a score report, details on how to apply for CISM certification.

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 the total scaled score cannot be determined by calculating either a simple or weighted average of the subscores.

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. Representations of CISM exam questions are available at www.isaca.org/cismassessment.

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 the CISM continuing professional education (CPE) policy requirements. 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 successfully completed the CISM exam and meet the following work experience requirements.

Five or more years of information security work experience, with a minimum of three 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]

Candidate's Guide to the CISM® Exam and Certification

For example, an applicant holding either a CISA or CISSP certification will qualify for the maximum two-year experience substitution. However, the applicant also must possess a minimum of three years of information security management work experience in three of the five job practice areas.

Exception: Two years as a full-time instructor teaching the management of information security can be substituted for every one year of information security management work experience.

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 a complete application for CISM certification is not submitted within five years from the passing date of the exam, retaking and passing the exam is required.

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, and attain and report a minimum of 120 CPE hours for a three-year reporting period. The CISM CPE policy (www.isaca.org/cismcpepolicy) requires the attainment of CPE hours over an annual and three-year reporting period. .
- Submit annual CPE maintenance fees in full to ISACA International Headquarters.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with the ISACA Code of Professional Ethics.

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

ISACA Code of Professional Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders. 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. The ISACA Code of Professional Ethics can be viewed online at www.isaca.org/ethics.

Revocation of CISM Certification

The CISM Certification Committee 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 CPE policy
- Violating any provision of the ISACA Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CISM exam or the certification process

Candidate's Guide to the CISM® Exam and Certification

Description of CISM Job Practice Areas CISM Task and Knowledge Statements

CONTENT AREA (Domain)
1. Information Security Governance —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.
Task Statements — <i>Develop, or be part of the development of, an IT governance framework that includes the following responsibilities and tasks:</i>
1.1 Develop an information security strategy aligned with business goals and objectives.
1.2 Align information security strategy with corporate governance.
1.3 Develop business cases justifying investment in information security.
1.4 Identify current and potential legal and regulatory requirements affecting information security.
1.5 Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
1.6 Obtain senior management commitment to information security.
1.7 Define roles and responsibilities for information security throughout the organization.
1.8 Establish internal and external reporting and communication channels that support information security.
Knowledge Statements
1.1 Knowledge of business goals and objectives
1.2 Knowledge of information security concepts
1.3 Knowledge of the components that comprise an information security strategy (e.g., processes, people, technologies, architectures)
1.4 Knowledge of the relationship between information security and business functions
1.5 Knowledge of the scope and charter of information security governance
1.6 Knowledge of the concepts of corporate and information security governance
1.7 Knowledge of methods of integrating information security governance into the overall enterprise governance framework
1.8 Knowledge of budgetary planning strategies and reporting methods
1.9 Knowledge of business case development
1.10 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
1.11 Knowledge of regulatory requirements and their potential business impact from an information security standpoint
1.12 Knowledge of common liability management strategies and insurance options (e.g., crime or fidelity insurance, business interruptions)
1.13 Knowledge of third-party relationships and their impact on information security (e.g., in cases of mergers and acquisitions)
1.14 Knowledge of methods used to obtain senior management commitment to information security
1.15 Knowledge of the establishment and operation of an information security steering group
1.16 Knowledge of information security management roles, responsibilities and general organizational structures
1.17 Knowledge of approaches for linking policies to enterprise business objectives
1.18 Knowledge of generally accepted international standards for information security management
1.19 Knowledge of centralized and distributed methods of coordinating information security activities
1.20 Knowledge of methods for establishing reporting and communication channels throughout an organization
2. Information Risk Management Identify and manage information security risks to achieve business objectives.
Task Statements
2.1 Establish a process for information asset classification and ownership.
2.2 Implement a systematic and structured information risk assessment process.
2.3 Ensure that business impact assessments are conducted periodically.
2.4 Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
2.5 Identify and periodically evaluate information security controls and countermeasures to mitigate risks to acceptable levels.
2.6 Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., development, procurement and employment life cycles).
2.7 Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Candidate's Guide to the CISM® Exam and Certification

CONTENT AREA (Domain)	
2. Information Risk Management (continued)	
Knowledge Statements	
2.1	Knowledge of required components for establishing an information classification schema consistent with business objectives (including the identification of assets)
2.2	Knowledge of the components of information ownership schema (including drivers of the schema such as roles and responsibilities)
2.3	Knowledge of information threats, vulnerabilities and exposures
2.4	Knowledge of information resource valuation methodologies
2.5	Knowledge of risk assessment and analysis methodologies (including measurability, repeatability and documentation)
2.6	Knowledge of factors used to determine risk reporting frequency and requirements
2.7	Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events on the business
2.8	Knowledge of baseline modeling and its relationship to risk-based assessments of control requirements
2.9	Knowledge of information security controls and countermeasures
2.10	Knowledge of methods of analyzing effectiveness of information security controls and countermeasures
2.11	Knowledge of risk mitigation strategies used in defining security requirements for information resources
2.12	Knowledge of gap analysis to assess generally accepted standards of good practice for information security management against the current state
2.13	Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks to acceptable levels
2.14	Knowledge of life cycle-based risk management principles and practices
3. Information Security Program Development—Create and maintain a program to implement the information security strategy.	
Task Statements	
3.1	Develop and maintain plans to implement the information security strategy.
3.2	Specify the activities to be performed within the information security program.
3.3	Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).
3.4	Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
3.5	Ensure the development of information security architectures (e.g., people, processes, technology).
3.6	Establish, communicate and maintain information security policies that support the security strategy.
3.7	Design and develop a program for information security awareness, training and education.
3.8	Ensure the development, communication and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
3.9	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).
3.10	Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
3.11	Establish metrics to evaluate the effectiveness of the information security program.
Knowledge Statements	
3.1	Knowledge of methods to interpret strategies into manageable and maintainable plans for implementing information security
3.2	Knowledge of the types of activities required within an information security program
3.3	Knowledge of methods for managing the implementation of the information security program
3.4	Knowledge of planning, designing, developing, testing and implementing information security controls
3.5	Knowledge of methods to align information security program requirements with those of other assurance functions (e.g., physical, HR, quality, IT)
3.6	Knowledge of how to identify internal and external resources and skills requirements (e.g., finances, people, equipment, systems)
3.7	Knowledge of resources and skills acquisition (e.g., project budgeting, employment of contract staff, equipment purchase)
3.8	Knowledge of information security architectures (e.g., logical architectures and physical architectures) and their deployment
3.9	Knowledge of security technologies and controls (e.g., cryptographic techniques, access controls, monitoring tools)
3.10	Knowledge of the process for developing information security policies that meet and support enterprise business objectives
3.11	Knowledge of content for information security awareness, training and education across the enterprise (e.g., general security awareness, writing secure code, operating security controls)
3.12	Knowledge of methods to identify activities to close the gap between proficiency levels and skill requirements
3.13	Knowledge of activities to foster a positive security culture and behavior
3.14	Knowledge of the uses of and differences between policies, standards, procedures, guidelines and other documentation

Candidate's Guide to the CISM® Exam and Certification

CONTENT AREA (Domain)
3. Information Security Program Development (continued)
3.15 Knowledge of process for linking policies to enterprise business objectives
3.16 Knowledge of methods to develop, implement, communicate and maintain information security policies, standards, procedures, guidelines and other documentation
3.17 Knowledge of methods of integrating information security requirements into organizational processes (e.g., change control, mergers and acquisitions)
3.18 Knowledge of life cycle methodologies and activities (e.g., development, employment, procurement)
3.19 Knowledge of processes for incorporating security requirements into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties)
3.20 Knowledge of methods and techniques to manage third-party risks (e.g., service level agreements, contracts, due diligence, suppliers, subcontractors)
3.21 Knowledge of the design, development and implementation of information security metrics
3.22 Knowledge of certifying and accrediting the compliance of business applications and infrastructures to business needs
3.23 Knowledge of methods for ongoing evaluation of the effectiveness and applicability of information security controls (e.g., vulnerability testing, assessment tools)
3.24 Knowledge of methods of tracking and measuring the effectiveness and currency of information security awareness, training and education
3.25 Knowledge of methods of sustaining the information security program (e.g., succession planning, allocation of jobs, documentation of the program)
4. Information Security Program Management—Oversee and direct information security activities to execute the information security program.
Task Statements
4.1 Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
4.2 Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
4.3 Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed.
4.4 Ensure that information security is an integral part of the systems development process.
4.5 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).
4.6 Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.
4.7 Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).
4.8 Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
4.9 Ensure that noncompliance issues and other variances are resolved in a timely manner.
Knowledge Statements
4.1 Knowledge of how to interpret information security policies and implement them
4.2 Knowledge of information security administrative processes and procedures (e.g., access controls, identity management, remote access)
4.3 Knowledge of methods for managing the enterprise's information security program through third parties (e.g., trade partners, contractors, joint ventures, outsourcing providers)
4.4 Knowledge of methods for managing the enterprise's information security program through security services providers
4.5 Knowledge of information security-related contract provisions (e.g., right to audit, confidentiality, nondisclosure)
4.6 Knowledge of methods to define and monitor security requirements in service level agreements (SLAs)
4.7 Knowledge of methods and approaches to providing continuous monitoring of security activities in the enterprise's infrastructure and business applications
4.8 Knowledge of management metrics to validate the information security program investment (e.g., data collection, periodic review, key performance indicators)
4.9 Knowledge of methods of testing the effectiveness and applicability of information security controls (e.g. penetration testing, password cracking, social engineering, assessment tools)
4.10 Knowledge of change and configuration management activities
4.11 Knowledge of the advantages/disadvantages of using internal/external assurance providers to perform information security reviews
4.12 Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information
4.13 Knowledge of external vulnerability reporting sources for information on potential impacts on information security in applications and infrastructure
4.14 Knowledge of events affecting security baselines that may require risk reassessments and changes to information security program elements
4.15 Knowledge of information security problem management practices

Candidate's Guide to the CISM® Exam and Certification

CONTENT AREA (Domain)
4.16 Knowledge of reporting requirements of systems and infrastructure security status
4.17 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)
5. Incident Management and Response —Plan, develop and manage a capability to detect, respond to and recover from information security incidents.
Task Statements
5.1 Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.
5.2 Establish escalation and communication processes and lines of authority.
5.3 Develop plans to respond to and document information security incidents.
5.4 Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
5.5 Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
5.6 Integrate information security incident response plans with the organization's disaster recovery plan (DRP) and business
5.7 Organize, train and equip teams to respond to information security incidents.
5.8 Periodically test and refine information security incident response plans.
5.9 Manage the response to information security incidents.
5.10 Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.
Knowledge Statements
5.1 Knowledge of the components of an incident response capability
5.2 Knowledge of recovery planning and business continuity planning
5.3 Knowledge of information incident management practices
5.4 Knowledge of disaster recovery testing for infrastructure and critical business applications
5.5 Knowledge of events that trigger incident response
5.6 Knowledge of methods of containing damage
5.7 Knowledge of notification and escalation processes for effective security management
5.8 Knowledge of the role of individuals in identifying and managing security incidents
5.9 Knowledge of crisis communications
5.10 Knowledge of methods identifying business resources essential to recovery
5.11 Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams
5.12 Knowledge of forensic requirements for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)
5.13 Knowledge used to document incidents and subsequent actions
5.14 Knowledge of internal and external reporting requirements
5.15 Knowledge of postincident review practices and investigative methods to identify causes and determine corrective actions
5.16 Knowledge of techniques for quantifying damages, costs and other business impacts arising from security incidents
5.17 Knowledge of recovery time objective (RTO) and its relationship to business continuity planning objectives and processes



Prepare for the **2011 CISM Exams**

2011 CISM Review Resources for Exam Preparation and Professional Development

Successful Certified Information Security Manager® (CISM®) exam candidates have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates. These include:

Study Aids

- *CISM Review Manual 2011*
- *CISM Review Questions, Answers & Explanations Manual 2011*
- *CISM Review Questions, Answers & Explanations Manual 2011 Supplement*
- CISM Practice Question Database v11

To order, visit www.isaca.org/cismbooks.

Review Courses

- Chapter-sponsored review courses

To find or register for a course in your region, visit www.isaca.org/cismreview.



ISBN 978-1-60420-158-1



9 781604 201581