2013

Candidate's Guide to the CISM® Exam and Certification

CISM® Certified Information Security Manager®

An ISACA® Certification

ISACA®

Trust in, and value from, information systems

CISM Exams 2013—Important Date Information

Exam Date—8 June 2013

Early registration deadline:	13 February 2013
Final registration deadline:	12 April 2013
Exam registration changes:	Between 13 April and 26 April, charged a US $50 fee, with no changes accepted after 26 April 2013
Refunds:	By 12 April 2013, charged a US $100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 26 April 2013, charged a US $50 processing fee. Requests received from 27 April through 24 May 2013, charged a US $100 processing fee. After 24 May 2013, no deferrals will be permitted.

Exam Date—14 December 2013

Early registration deadline:	21 August 2013
Final registration deadline:	25 October 2013
Exam registration changes:	Between 26 October and 1 November, charged a US $50 fee, with no changes accepted after 1 November 2013
Refunds:	By 25 October 2013, charged a US $100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 25 October 2013, charged a US $50 processing fee. Requests received from 26 October through 27 November 2013, charged a US $100 processing fee. After 27 November 2013 no deferrals will be permitted.

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

ISBN 978-1-60420-333-2
2013 Candidate's Guide to the CISM® Exam and Certification
Printed in the United States of America

Table of Contents

ISACA®
With more than 100,000 constituents in 180 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®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT® framework. COBIT helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA and the CISM Certification Committee have designed the *2013 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

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *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

ANSI Accredited Program
PERSONNEL CERTIFICATION
#0694
ISO/IEC 17024

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 CISMs 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 four domain areas. 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 CISMs 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 (24%)**
- **Information Risk Management and Compliance (33%)**
- **Information Security Program Development and Management (25%)**
- **Information Security Incident Management (18%)**

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 2013.*

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 utlizes 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 or the content of the exam, should contact ISACA international headquarters by letter or by email (*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. Only those comments received by ISACA during the first 2 weeks after the exam administration will be considered in the final scoring process of the exam.

Admission Ticket

Approximately two to three weeks prior to the CISM exam date, candidates will be sent a physical admission ticket and an e-ticket from ISACA. Exam candidates can also download a copy of the admission ticket at *www.isaca.org* > MyISACA page of the web site. 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 email to the current postal mailing and email 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 email 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. Consideration for reasonable alterations in scheduling, exam format, presentation, and allowance of food or drink at the exam site must be requested. Documented disability requests must be accompanied by a doctor's note. Requests for a religious requirement must be accompanied by a note from the candidate's religious leader. Unless requested, **no food or drink is allowed at any exam site**. Requests for consideration must be submitted to ISACA International Headquarters in writing, accompanied by appropriate documentation, no later than 12 April 2013 for the June 2013 exam and 25 October 2013 for the December 2013 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. As exam venues vary, every attempt will be made to make the climate control comfortable at each exam venue. Candidates may want to dress to their own comfort level.
- 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.
- 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.

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 during the registration process, an email message containing the candidate's pass/fail status and score will be sent to the candidate. This email 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 email 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, rescores 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 $75 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. To gain a better understanding of the types of questions that might appear on the exam and how these questions are developed, refer to the CISM Item Writing Guide available at *www.isaca.org/itemwriter*. 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.** Please note that decisions on applications are not final as there is an appeal process for certification application denials. Inquiries regarding denials of certification can be sent to *certification@isaca.org*. Once certified, the new CISM will receive a certificate and CISM certification pin. 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. A processing fee of US $50 must accompany your CISM Application for Certification.

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]

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 four job practice areas.

Exception: Two years as a full-time university 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. For more details visit the CISM CPE policy at *www.isaca.org/cismcpepolicy*.
- 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. All certificates are owned by ISACA. If an individual is approved for certification and subsequently revoked, the individual must destroy the certificate.

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
- As of January 2013, all appeals resulting in reinstatement related to revocations more than 60 days old will require a US $50 reinstatement fee to be processed.

Description of CISM Job Practice Areas

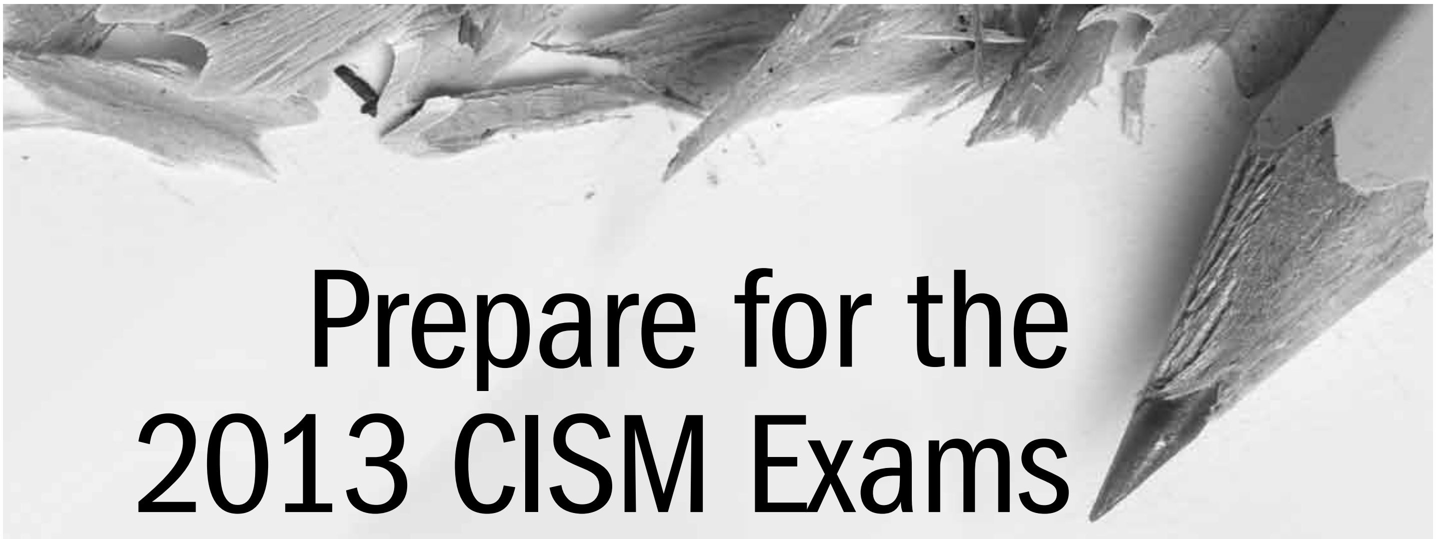
CISM Task and Knowledge Statements

CONTENT AREA (Domain)	
Domain 1—Information Security Governance (24%)—Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.	
Task Statements	
T1.1	Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
T1.2	Establish and maintain an information security governance framework to guide activities that support the information security strategy.
T1.3	Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
T1.4	Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.
T1.5	Develop business cases to support investments in information security.
T1.6	Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.
T1.7	Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
T1.8	Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
T1.9	Establish, monitor, evaluate and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.
Knowledge Statements	
KS1.1	Knowledge of methods to develop an information security strategy
KS1.2	Knowledge of the relationship among information security and business goals, objectives, functions, processes and practices
KS1.3	Knowledge of methods to implement an information security governance framework
KS1.4	Knowledge of the fundamental concepts of governance and how they relate to information security
KS1.5	Knowledge of methods to integrate information security governance into corporate governance
KS1.6	Knowledge of internationally recognized standards, frameworks and best practices related to information security governance and strategy development
KS1.7	Knowledge of methods to develop information security policies
KS1.8	Knowledge of methods to develop business cases
KS1.9	Knowledge of strategic budgetary planning and reporting methods
KS1.10	Knowledge of the internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) and how they impact the information security strategy
KS1.11	Knowledge of methods to obtain commitment from senior management and support from other stakeholders for information security
KS1.12	Knowledge of information security management roles and responsibilities
KS1.13	Knowledge of organizational structures and lines of authority
KS1.14	Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
KS1.15	Knowledge of methods to select, implement and interpret metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])
Domain 2—Information Risk Management and Compliance (33%)—Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.	
Task Statements	
T2.1	Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
T2.2	Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

CONTENT AREA (Domain)	
Domain 2—Information Risk Management and Compliance ***(cont.)***	
T2.3	Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically and consistently to identify risk to the organization's information.
T2.4	Determine appropriate risk treatment options to manage risk to acceptable levels.
T2.5	Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
T2.6	Identify the gap between current and desired risk levels to manage risk to an acceptable level.
T2.7	Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
T2.8	Monitor existing risk to ensure that changes are identified and managed appropriately.
T2.9	Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.
Knowledge Statements	
KS2.1	Knowledge of methods to establish an information asset classification model consistent with business objectives
KS2.2	Knowledge of methods used to assign the responsibilities for and ownership of information assets and risk
KS2.3	Knowledge of methods to evaluate the impact of adverse events on the business
KS2.4	Knowledge of information asset valuation methodologies
KS2.5	Knowledge of legal, regulatory, organizational and other requirements related to information security
KS2.6	Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities
KS2.7	Knowledge of events that may require risk reassessments and changes to information security program elements
KS2.8	Knowledge of information threats, vulnerabilities and exposures and their evolving nature
KS2.9	Knowledge of risk assessment and analysis methodologies
KS2.10	Knowledge of methods used to prioritize risk
KS2.11	Knowledge of risk reporting requirements (for example, frequency, audience, components)
KS2.12	Knowledge of methods used to monitor risk
KS2.13	Knowledge of risk treatment strategies and methods to apply them
KS2.14	Knowledge of control baseline modeling and its relationship to risk-based assessments
KS2.15	Knowledge of information security controls and countermeasures and the methods to analyze their effectiveness and efficiency
KS2.16	Knowledge of gap analysis techniques as related to information security
KS2.17	Knowledge of techniques for integrating risk management into business and IT processes
KS2.18	Knowledge of compliance reporting processes and requirements
KS2.19	Knowledge of cost/benefit analysis to assess risk treatment options
Domain 3—Information Security Program Development and Management (25%)—Establish and manage the information security program in alignment with the information security strategy.	
Task Statements	
T3.1	Establish and maintain the information security program in alignment with the information security strategy.
T3.2	Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes.
T3.3	Identify, acquire, manage and define requirements for internal and external resources to execute the information security program.
T3.4	Establish and maintain information security architectures (people, process, technology) to execute the information security program.
T3.5	Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
T3.6	Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.

CONTENT AREA (Domain)	
Domain 3—Information Security Program Development and Management ***(cont.)***	
T3.7	Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization’s security baseline.
T3.8	Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization’s security baseline.
T3.9	Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.
Knowledge Statements	
KS3.1	Knowledge of methods to align information security program requirements with those of other business functions
KS3.2	Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources
KS3.3	Knowledge of information security technologies, emerging trends, (for example, cloud computing, mobile computing) and underlying concepts
KS3.4	Knowledge of methods to design information security controls
KS3.5	Knowledge of information security architectures (for example, people, process, technology) and methods to apply them
KS3.6	Knowledge of methods to develop information security standards, procedures and guidelines
KS3.7	Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines
KS3.8	Knowledge of methods to establish and maintain effective information security awareness and training programs
KS3.9	Knowledge of methods to integrate information security requirements into organizational processes
KS3.10	Knowledge of methods to incorporate information security requirements into contracts and third-party management processes
KS3.11	Knowledge of methods to design, implement and report operational information security metrics
KS3.12	Knowledge of methods for testing the effectiveness and applicability of information security controls
Domain 4—Information Security Incident Management (18%)—Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.	
Task Statements	
T4.1	Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents.
T4.2	Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
T4.3	Develop and implement processes to ensure the timely identification of information security incidents.
T4.4	Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
T4.5	Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.
T4.6	Organize, train and equip teams to effectively respond to information security incidents in a timely manner.
T4.7	Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.
T4.8	Establish and maintain communication plans and processes to manage communication with internal and external entities.
T4.9	Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
T4.10	Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan.
Knowledge Statements	
KS4.1	Knowledge of the components of an incident response plan
KS4.2	Knowledge of incident management concepts and practices
KS4.3	Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan
KS4.4	Knowledge of incident classification methods
KS4.5	Knowledge of damage containment methods

CONTENT AREA (Domain)	
Domain 4—Information Security Incident Management ***(cont.)***	
KS4.6	Knowledge of notification and escalation processes
KS4.7	Knowledge of the roles and responsibilities in identifying and managing information security incidents
KS4.8	Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams
KS4.9	Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (for example, admissibility, quality and completeness of evidence, chain of custody)
KS4.10	Knowledge of internal and external incident reporting requirements and procedures
KS4.11	Knowledge of postincident review practices and investigative methods to identify root causes and determine corrective actions
KS4.12	Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents
KS4.13	Knowledge of technologies and processes that detect, log and analyze information security events
KS4.14	Knowledge of internal and external resources available to investigate information security incidents



Prepare for the 2013 CISM Exams

2013 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 2013*
- *CISM® Review Questions, Answers & Explanations Manual 2012*
- *CISM® Review Questions, Answers & Explanations Manual 2012 Supplement*
- *CISM® Review Questions, Answers & Explanations Manual 2013 Supplement*
- CISM® Practice Question Database v13

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*.

ISACA®
Trust in, and value from, information systems

CISM® Certified Information Security Manager®
An ISACA® Certification

ISBN 978-1-60420-333-2
90000>
9 781604 203332

DOC: 2013 CISM Candidates Guide
Version: V2
Update: 2012-1201