



CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL[™]

2012 Candidate's Guide to the
CRISC[™] Exam and Certification

Candidate's Guide to the CRISC™ Exam and Certification

CRISC Exams 2012— Important Date Information

Exam Date—9 June 2012

Early registration deadline:	8 February 2012
Final registration deadline:	4 April 2012
Exam registration changes:	Between 14 April and 20 April, charged a US \$50 fee, with no changes accepted after 20 April 2012
Refunds:	By 13 April 2012, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 20 April 2012, charged a US \$50 processing fee. Requests received from 21 April through 24 May 2012, charged a US \$100 processing fee. After 24 May 2012, no deferrals will be permitted.

Exam Date—8 December 2012

Early registration deadline:	15 August 2012
Final registration deadline:	3 October 2012
Exam registration changes:	Between 6 October and 12 October, charged a US \$50 fee, with no changes accepted after 12 October 2012
Refunds:	By 5 October 2012, charged a US \$100 processing fee, with no refunds after that date
Deferrals:	Requests received on or before 12 October 2012, charged a US \$50 processing fee. Requests received from 13 October through 21 November 2012, charged a US \$100 processing fee. After 21 November 2012 no deferrals will be permitted.

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

ISBN 978-1-60420-232-8
2012 Candidate's Guide to the CRISC™ Exam and Certification
Printed in the United States of America

Table of Contents

Overview	3
The CRISC Exam	3
Preparing for the CRISC Exam	3
Administration of the CRISC Exam	4
Scoring the CRISC Exam	6
Types of Questions on the CRISC Exam	6
Application for CRISC Certification.....	6
Requirements for Initial CRISC Certification.....	6
Requirements for Maintaining CRISC Certification.....	7
ISACA Code of Professional Ethics.....	7
Revocation of CRISC Certification	7
CRISC 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®), 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 COBIT®, which 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 CRISC Certification Committee have designed the *2012 Candidate's Guide to the CRISC™ Exam and Certification* as a guide to those pursuing the CRISC 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 CRISC exam.

Reservation of Rights

Copyright © 2011 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 CRISC™ Exam and Certification

Overview

The mark of excellence for a professional certification program is the value and recognition it bestows on the individual who achieves it. The Certified in Risk and Information Systems Control (CRISC) program, sponsored by ISACA, recognizes a wide range of professionals for their knowledge of enterprise risk and their ability to design, implement, monitor and maintain information systems (IS) controls to mitigate such risk.

The CRISC certification, CRISC™, pronounced “see-risk,” is designed for IT professionals who have hands-on experience with risk identification, assessment and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance.

The CRISC designation will not only certify professionals who have knowledge and experience identifying and evaluating entity-specific risk, but also aid them in helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls.

The technical skills and practices that CRISC promotes and evaluates are the building blocks of success in the field. Possessing the CRISC designation demonstrates proficiency and is the basis for measurement in the profession. With a growing demand for professionals possessing risk and control skills, CRISC has positioned itself to be the preferred certification program by individuals and enterprises around the world. CRISC certification signifies commitment to serving an enterprise and the chosen profession with distinction.

The CRISC Exam

Development/Description of the CRISC Exam

The CRISC Certification Committee oversees the development of the exam and ensures the currency of its content. Questions for the CRISC exam were developed through a comprehensive process designed to enhance 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 CRISC Certification Committee for review.

A job practice serves as the basis for the exam and the experience requirements to earn the CRISC 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 task and knowledge statements depict the tasks performed by CRISCs and the knowledge required to perform these tasks. Exam candidates will be tested based on their practical knowledge associated with performing these tasks.

Content of the CRISC Exam

The CRISC exam measures an individual's ability and knowledge as they pertain to the performance of the CRISC task statements (see pages 8-11). The content of the exam is modified to reflect changes in technology and practices.

- **Domain 1—Risk Identification, Assessment and Evaluation (31 percent):** Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.
- **Domain 2—Risk Response (17 percent):** Develop and implement risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives.
- **Domain 3—Risk Monitoring (17 percent):** Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy.
- **Domain 4—Information Systems Control Design and Implementation (17 percent):** Design and implement information systems controls in alignment with the organization's risk appetite and tolerance levels to support business objectives.
- **Domain 5—Information Systems Control Monitoring and Maintenance (18 percent):** Monitor and maintain information systems controls to ensure that they function effectively and efficiently.

Note: The percentages listed above 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 twice each year in June and December during a four-hour session. Currently, the CRISC exam is offered in English only.

Preparing for the CRISC Exam

Passing the CRISC 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/criscbbooks to view the ISACA study aids that can help you prepare for the exam. Order early since 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.

The *CRISC™ Review Manual 2012* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The 2012 edition has been developed by global SMEs to assist candidates in understanding essential concepts of the CRISC job practice areas. In addition, ISACA also offers the *CRISC™ Review Questions, Answers & Explanations Manual 2011 and 2012 Supplement*. For complete descriptions, or to place an order, please visit www.isaca.org/criscbbooks.

Candidate's Guide to the CRISC™ Exam and Certification

CRISC exam candidates should be familiar with the terminology and concepts in ISACA's intellectual property and other credible sources. For how best to prepare for the exam, see www.isaca.org/criscfaq.

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

Administration of the CRISC Exam

ISACA utilizes an internationally recognized professional testing agency to assist in the construction, administration and scoring of the CRISC 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 e-mail (exam@isaca.org). These comments or concerns are to be received by ISACA within two 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 two 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 CRISC 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 CRISC exam. With the exception of contact information changes, candidates are not to write on the admission ticket.

Please note: 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 acceptable government-issued identification (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 printout 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 the registration fee. An admission ticket can be used only 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 4 April 2012 for the June 2012 exam and 3 October 2012 for the December 2012 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 INTO 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 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 the registration fee.

Observe the Test Center's Rules

- Candidates will not be admitted to a test 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.

Candidate's Guide to the CRISC™ Exam and Certification

- Candidates are not allowed to bring any type of communication devices (i.e., cell phones, PDAs, BlackBerry®) 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 CRISC Certification Committee.

The complete Personal Belongings Policy is available at www.isaca.org/criscbelongings. 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 correctly entered or scores may be delayed or incorrectly reported.
- A proctor speaking the primary language used at each test center is available.
- 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 not to mark more than one answer per question and must 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. Scores 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 more than 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 that a candidate marks 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 CRISC 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 test center. The testing agency will provide the CRISC Certification Committee with records regarding such irregularities for their 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 CRISC Exam

The CRISC 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. ISACA uses and reports scores on a common scale from 200 to 800. 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 candidate must receive a score of 450 or higher to pass the exam. A score of 450 represents a minimum consistent standard of knowledge as established by the CRISC Certification Committee. A candidate receiving a passing score may then apply for certification if all other requirements are met.

Candidate's Guide to the CRISC™ Exam and Certification

The CRISC exam contains some questions that 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 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. Successful candidates will receive, along with a score report, details on how to apply for CRISC 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 \$75 must accompany each request.

Types of Questions on the CRISC Exam

CRISC exam questions are developed with the intent of measuring and testing practical knowledge and the application of concepts, standards and practices. All questions are designed with one best answer.

Every CRISC 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 may also 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 CRISC 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.

Application for CRISC Certification

Passing the exam does not mean a candidate is a CRISC. Once a candidate passes the CRISC 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. A processing fee of US \$50 must accompany your CRISC Application for Certification. **Candidates are not certified, and cannot use the CRISC 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 CRISC will receive a certificate and a CRISC 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 CRISC status.

Requirements for Initial CRISC Certification

Certification is granted initially to individuals who have successfully completed the CRISC exam and meet the following work experience requirements in the fields of risk management and IS control. A minimum of at least three (3) years of cumulative work experience performing the tasks of a CRISC professional across at least three (3) CRISC domains is required for certification. There are no substitutions or experience waivers.

Experience must have been gained within the 10-year period preceding the date of the application for CRISC certification or within five (5) years from the date of initially passing the exam. If a complete application for CRISC certification is not submitted within five (5) years from the passing date of the exam, retaking and passing the exam is required.

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

Adherence to the Code of Professional Ethics. Members of ISACA and/or holders of the CRISC designation agree to a Code of Professional Ethics to guide professional and personal conduct. The code of Professional Ethics can be viewed at www.isaca.org/ethics.

Candidate's Guide to the CRISC™ Exam and Certification

Requirements for Maintaining CRISC Certification

CRISCs 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 CRISC CPE policy at www.isaca.org/crisccepolicy.
- Submit annual CPE hours and certification 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 CRISC 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 CRISC Certification

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

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

Candidate's Guide to the CRISC™ Exam and Certification

CRISC Task and Knowledge Statements

DOMAIN	
Domain 1—Risk Identification, Assessment and Evaluation —Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.	
Domain 1—Task Statements	
1.1	Collect information and review documentation to ensure that risk scenarios are identified and evaluated.
1.2	Identify legal, regulatory and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.
1.3	Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
1.4	Create and maintain a risk register to ensure that all identified risk factors are accounted for.
1.5	Assemble risk scenarios to estimate the likelihood and impact of significant events to the organization.
1.6	Analyze risk scenarios to determine their impact on business objectives.
1.7	Develop a risk awareness program and conduct training to ensure that stakeholders understand risk and contribute to the risk management process and to promote a risk-aware culture.
1.8	Correlate identified risk scenarios to relevant business processes to assist in identifying risk ownership.
1.9	Validate risk appetite and tolerance with senior leadership and key stakeholders to ensure alignment.
Domain 1—Knowledge Statements	
1.1	Knowledge of standards, frameworks and leading practices related to risk identification, assessment and evaluation
1.2	Knowledge of techniques for risk identification, classification, assessment and evaluation
1.3	Knowledge of quantitative and qualitative risk evaluation methods
1.4	Knowledge of business goals and objectives
1.5	Knowledge of organizational structures
1.6	Knowledge of risk scenarios related to business processes and initiatives
1.7	Knowledge of business information criteria
1.8	Knowledge of threats and vulnerabilities related to business processes and initiatives
1.9	Knowledge of information systems architecture (e.g., platforms, networks, applications, databases and operating systems)
1.10	Knowledge of information security concepts
1.11	Knowledge of threats and vulnerabilities related to third-party management
1.12	Knowledge of threats and vulnerabilities related to data management
1.13	Knowledge of threats and vulnerabilities related to the system development life cycle
1.14	Knowledge of threats and vulnerabilities related to project and program management
1.15	Knowledge of threats and vulnerabilities related to business continuity and disaster recovery management
1.16	Knowledge of threats and vulnerabilities related to management of IT operations
1.17	Knowledge of the elements of a risk register
1.18	Knowledge of risk scenario development tools and techniques
1.19	Knowledge of risk awareness training tools and techniques
1.20	Knowledge of principles of risk ownership
1.21	Knowledge of current and forthcoming laws, regulations and standards
1.22	Knowledge of threats and vulnerabilities associated with emerging technologies

Candidate's Guide to the CRISC™ Exam and Certification

DOMAIN
Domain 2—Risk Response —Develop and implement risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives.
Domain 2—Task Statements
2.1 Identify and evaluate risk response options and provide management with information to enable risk response decisions.
2.2 Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy.
2.3 Apply risk criteria to assist in the development of the risk profile for management approval.
2.4 Assist in the development of risk response action plans to address risk factors identified in the organizational risk profile.
2.5 Assist in the development of business cases supporting the investment plan to ensure that risk responses are aligned with the identified business objectives.
Domain 2—Knowledge Statements
2.1 Knowledge of standards, frameworks and leading practices related to risk response
2.2 Knowledge of risk response options
2.3 Knowledge of cost-benefit analysis and return on investment (ROI)
2.4 Knowledge of risk appetite and tolerance
2.5 Knowledge of organizational risk management policies
2.6 Knowledge of parameters for risk response selection
2.7 Knowledge of project management tools and techniques
2.8 Knowledge of portfolio, investment and value management
2.9 Knowledge of exception management
2.10 Knowledge of residual risk
Domain 3—Risk Monitoring —Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy.
Domain 3—Task Statements
3.1 Collect and validate data that measure key risk indicators (KRIs) to monitor and communicate their status to relevant stakeholders.
3.2 Monitor and communicate key risk indicators (KRIs) and management activities to assist relevant stakeholders in their decision-making process.
3.3 Facilitate independent risk assessments and risk management process reviews to ensure that they are performed efficiently and effectively.
3.4 Identify and report on risk, including compliance, to initiate corrective action and meet business and regulatory requirements.
Domain 3—Knowledge Statements
3.1 Knowledge of standards, frameworks and leading practices related to risk monitoring
3.2 Knowledge of principles of risk ownership
3.3 Knowledge of risk and compliance reporting requirements, tools and techniques
3.4 Knowledge of key performance indicators (KPIs) and key risk indicators (KRIs)
3.5 Knowledge of risk assessment methodologies
3.6 Knowledge of data extraction, validation, aggregation and analysis tools and techniques
3.7 Knowledge of various types of reviews of the organization's risk monitoring process (e.g., internal and external audits, peer reviews, regulatory reviews, quality reviews)

Candidate's Guide to the CRISC™ Exam and Certification

DOMAIN	
Domain 4—Information Systems Control Design and Implementation —Design and implement information systems controls in alignment with the organization's risk appetite and tolerance levels to support business objectives.	
Domain 4—Task Statements	
4.1	Interview process owners and review process design documentation to gain an understanding of the business process objectives.
4.2	Analyze and document business process objectives and design to identify required information systems controls.
4.3	Design information systems controls in consultation with process owners to ensure alignment with business needs and objectives.
4.4	Facilitate the identification of resources (e.g., people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
4.5	Monitor the information systems control design and implementation process to ensure that it is implemented effectively and within time, budget and scope.
4.6	Provide progress reports on the implementation of information systems controls to inform stakeholders and to ensure that deviations are promptly addressed.
4.7	Test information systems controls to verify effectiveness and efficiency prior to implementation.
4.8	Implement information systems controls to mitigate risk.
4.9	Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of information systems control performance in meeting business objectives.
4.10	Assess and recommend tools to automate information systems control processes.
4.11	Provide documentation and training to ensure that information systems controls are effectively performed.
4.12	Ensure that all controls are assigned control owners to establish accountability.
4.13	Establish control criteria to enable control life cycle management.
Domain 4—Knowledge Statements	
4.1	Knowledge of standards, frameworks and leading practices related to information systems control design and implementation
4.2	Knowledge of business process review tools and techniques
4.3	Knowledge of testing methodologies and practices related to information systems control design and implementation
4.4	Knowledge of control practices related to business processes and initiatives
4.5	Knowledge of the information systems architecture (e.g., platforms, networks, applications, databases and operating systems)
4.6	Knowledge of controls related to information security
4.7	Knowledge of controls related to third-party management
4.8	Knowledge of controls related to data management
4.9	Knowledge of controls related to the system development life cycle
4.10	Knowledge of controls related to project and program management
4.11	Knowledge of controls related to business continuity and disaster recovery management
4.12	Knowledge of controls related to management of IT operations
4.13	Knowledge of software and hardware certification and accreditation practices
4.14	Knowledge of the concept of control objectives
4.15	Knowledge of governance, risk and compliance (GRC) tools
4.16	Knowledge of tools and techniques to educate and train users

Candidate's Guide to the CRISC™ Exam and Certification

DOMAIN
Domain 5—Information Systems Control Monitoring and Maintenance —Monitor and maintain information systems controls to ensure that they function effectively and efficiently.
<i>Domain 5—Task Statements</i>
5.1 Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls.
5.2 Collect information and review documentation to identify information systems control deficiencies.
5.3 Review information systems policies, standards and procedures to verify that they address the organization's internal and external requirements.
5.4 Assess and recommend tools and techniques to automate information systems control verification processes.
5.5 Evaluate the current state of information systems processes using a maturity model to identify the gaps between current and targeted process maturity.
5.6 Determine the approach to correct information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately considered and remediated.
5.7 Maintain sufficient, adequate evidence to support conclusions on the existence and operating effectiveness of information systems controls.
5.8 Provide information systems control status reporting to relevant stakeholders to enable informed decision making.
<i>Domain 5—Knowledge Statements</i>
5.1 Knowledge of standards, frameworks and leading practices related to information systems control monitoring and maintenance
5.2 Knowledge of enterprise security architecture
5.3 Knowledge of monitoring tools and techniques
5.4 Knowledge of maturity models
5.5 Knowledge of control objectives, activities and metrics related to IT operations and business processes and initiatives
5.6 Knowledge of control objectives, activities and metrics related to incident and problem management
5.7 Knowledge of security testing and assessment tools and techniques
5.8 Knowledge of control objectives, activities and metrics related to information systems architecture (platforms, networks, applications, databases and operating systems)
5.9 Knowledge of control objectives, activities and metrics related to information security
5.10 Knowledge of control objectives, activities and metrics related to third-party management
5.11 Knowledge of control objectives, activities and metrics related to data management
5.12 Knowledge of control objectives, activities and metrics related to the system development life cycle
5.13 Knowledge of control objectives, activities and metrics related to project and program management
5.14 Knowledge of control objectives, activities and metrics related to software and hardware certification and accreditation practices
5.15 Knowledge of control objectives, activities and metrics related to business continuity and disaster recovery management
5.16 Knowledge of applicable laws and regulations



Prepare for the 2012 CRISC Exams

2012 CRISC Review Resources for Exam Preparation and Professional Development

Successful Certified in Risk and Information Systems Control™ (CRISC™) 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

- *CRISC™ Review Manual 2012*
- *CRISC™ Review Questions, Answers & Explanations Manual 2011*
- *CRISC™ Review Questions, Answers & Explanations Manual 2012 Supplement*

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

Review Courses

- CRISC boot camps may be offered in conjunction with ISACA conferences as pre-conference workshops. For information, visit www.isaca.org/conferences.
- For CRISC review courses in your area, please refer to your chapter's web site at www.isaca.org/chapters.

