CISM® Review Questions, Answers & Explanations Manual

10th Edition

Certified Information Security Manager®
An ISACA® Certification

ISACA®

About ISACA

For more than 50 years, ISACA® (*www.isaca.org*) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. Among those credentials, ISACA advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control® (CRISC®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified Data Privacy Solutions Engineer™ (CDPSE™) credentials. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

Disclaimer

ISACA has designed and created *CISM Review Questions, Answers & Explanations Manual 10th Edition* primarily as an educational resource to assist individuals preparing to take the CISM certification exam. It was produced independently from the CISM exam and the CISM Certification Committee, which has had no responsibility for its content. Copies of past exams are not released to the public and were not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA publications assuring candidates' passage of the CISM exam.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums
Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

ISBN 978-1-60420-903-7
CISM® Review Questions, Answers & Explanations Manual 10th Edition
Printed in the United States of America

PREFACE

ISACA is pleased to offer the 1,000 questions in this *CISM® Review Questions, Answers & Explanations Manual 10th Edition*. The purpose of this manual is to provide the CISM candidate with sample questions and testing topics to help prepare and study for the CISM exam.

This manual consists of 1,000 multiple-choice study questions, answers and explanations, which are organized according to the newly revised (effective 2022) CISM job practice domains. These questions, answers and explanations are intended to introduce CISM candidates to the types of questions that may appear on the CISM exam. They are not actual questions from the exam. Some of these items appeared in previous editions of the *CISM® Review Questions, Answers & Explanations Manual*, but many have been rewritten or enhanced to be more representative of actual exam items and to provide further clarity or reflect a change in practice. The 1,000 questions are sorted by CISM domains. Additionally, 150 questions have been extracted to provide a sample exam with questions in the same proportion as the current CISM job practice. The candidate also may want to obtain a copy of the *CISM® Review Manual 16th Edition*, which provides the foundational knowledge of a CISM.

A job practice study is conducted at least every five years to ensure that the CISM certification is current and relevant. Further details regarding the new job practice can be found in the section titled New—CISM Job Practice.

ISACA has produced this publication as an educational resource to assist individuals preparing to take the CISM exam. It was produced independently from the CISM Certification Working Group, which has no responsibility for its content. Copies of past exams are not released to the public and are not made available to candidates. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA or IT Governance Institute publications assuring candidates' passage of the CISM exam.

ISACA wishes you success with the CISM exam. Your commitment to pursuing the leading certification for information security managers is exemplary, and we welcome your comments and suggestions on the use and coverage of this manual. Once you have completed the exam, please take a moment to complete the online evaluation that corresponds to this publication *(www.isaca.org/studyaidsevaluation)*. Your observations will be invaluable as new questions, answers and explanations are prepared.

Page intentionally left blank

ACKNOWLEDGMENTS

The *CISM® Review Questions, Answers & Explanations Manual 10th Edition* is the result of the collective efforts of many volunteers over the past several years. ISACA members from throughout the global information security management profession participated, generously offering their talents and expertise. This international team exhibited a spirit of selflessness that has become the hallmark of contributors to this valuable manual. Their participation and insight are truly appreciated.

We would like to acknowledge the 2021 CISM Quality Assurance Team for their hard work and dedication to updating and improving this manual.

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

NEW—CISM JOB PRACTICE

BEGINNING IN 2022, THE CISM EXAM WILL TEST THE NEW CISM JOB PRACTICE.

An international job practice analysis is conducted at least every five years or sooner to maintain the validity of the CISM certification program. A new job practice forms the basis of the CISM exam beginning in 2022.

The job practice focuses primarily on the current tasks performed and the knowledge used by CISMs. By gathering evidence of the current work practice of CISMs, ISACA is able to ensure that the CISM program continues to meet the high standards for the certification of professionals throughout the world.

The findings of the CISM job practice analysis are carefully considered and directly influence the development of new test specifications to ensure that the CISM exam reflects the most current best practices.

The new 2022 job practice reflects the areas of study to be tested. The following table compares it to the previous job practice. The complete CISM job practice can be found at *www.isaca.org/credentialing/cism/cism-job-practice-areas*.

Previous CISM Job Practice	New 2022 CISM Job Practice
Domain 1: Information Security Governance (24%)	**Domain 1: Information Security Governance (17%)**
Domain 2: Information Risk Management (30%)	**Domain 2: Information Security Risk Management (20%)**
Domain 3: Information Security Program Development and Management (27%)	**Domain 3: Information Security Program (33%)**
Domain 4: Information Security Incident Management (19%)	**Domain 4: Incident Management (30%)**

Page intentionally left blank

INTRODUCTION

The CISM exam evaluates a candidate's practical knowledge, including experience and application, of the job practice domains. We recommend that the exam candidate look to multiple resources to prepare for the exam, including the *CISM® Review Manual and Questions, Answers & Explanation (QAE) Manual* or the database, along with external publications. This section will cover some tips for studying for the exam and how best to use this QAE Manual in conjunction with other resources.

GETTING STARTED

Having adequate time to prepare for the CISM exam is critical. Most candidates spend between three and six months studying prior to taking the exam. Make sure you set aside a designated time each week to study, which you may wish to increase as your exam date approaches.

Developing a plan for your study efforts can also help you make the most effective use of your time prior to taking the exam.

ABOUT THIS MANUAL

The *CISM QAE Manual* provides questions similar to those found on the CISM exam. They are developed using the task and knowledge statements as described in the CISM job practice.

This manual consists of 1,000 multiple-choice questions, answers and explanations. These questions are selected and provided in two formats.

Questions Sorted by Domain

Questions, answers and explanations are provided (sorted) by the four CISM job practice domains. This allows the CISM candidate to refer to specific questions to evaluate comprehension of the topics covered within each domain. These questions are representative of CISM questions, although they are not actual exam items. They are provided to assist the CISM candidate in understanding the material in the *CISM® Review Manual 15th Edition* and to depict the type of question format typically found on the CISM exam. The numbers of questions, answers and explanations provided in the four domain chapters in this publication provide the CISM candidate with a maximum number of study questions.

Sample Exam

A random sample exam of 150 of the questions is also provided in this manual. **This exam is organized according to the domain percentages specified in the CISM job practice and used on the CISM exam:**

Information Security Governance	17 percent
Information Security Risk Management	20 percent
Information Security Program	33 percent
Incident Management	30 percent

Candidates are urged to use this sample exam and the answer sheets provided to simulate an actual exam. There are two primary ways this sample exam may be used. The first is as a pretest, which is taken prior to any additional study. The sample exam in the QAE Manual is the same length as the actual CISM exam, as opposed to the CISM

self-assessment, which is an abbreviated self-assessment tool. The pretest can help you to determine your domain weaknesses. It can also help to orient you to the types of questions you may encounter in your study and during the exam.

The second way to use the sample exam is as a posttest. This will help you to determine the effectiveness of your study efforts as you approach the exam date. The results of this posttest can help you to focus on domains and task/knowledge statements that may require some additional review prior to taking the exam.

Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. These sample exam questions are cross-referenced to the questions, answers and explanations by domain, so it is convenient to refer to the explanations of the correct answers. This publication is ideal to use in conjunction with the *CISM® Review Manual 16th Edition*.

It should be noted that the *CISM® Review Questions, Answers & Explanations Manual 10th Edition* has been developed to assist the CISM candidate in studying and preparing for the CISM exam. As you use this publication to prepare for the exam, please note that it covers a broad spectrum of information security management issues. Do not assume that reading and working the questions in this manual will fully prepare you for the exam. Because exam questions often relate to practical experience, it is recommended that you refer to your own experience and to other publications referred to in the *CISM® Review Manual 16th Edition*. These additional references are excellent sources of further detailed information and clarification. It is recommended that candidates identify the job practice domains in which they feel weak, or require a further understanding, and study accordingly.

Also, please note that this publication has been written using standard American English.

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 information security managerial principles and standards. All questions are presented in a multiple-choice format and are designed for one best answer.

The candidate is cautioned to read each question carefully. Many times a CISM exam question will require the candidate to choose the appropriate answer that is **MOST** likely or **BEST**, or the candidate may be asked to choose a practice or procedure that would be performed **FIRST** related to the other answers. In every case, the candidate is required to read the question carefully, eliminate known wrong answers and then make the best choice possible. Knowing that these types of questions are asked and how to study for them will go a long way toward answering them correctly. The best answer is one of the choices provided. There can be many potential solutions to the scenarios posed in the questions, depending on industry, geographical location, etc. It is advisable to consider the information provided in the question and to determine the best answer of the options provided.

Each CISM 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 also 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.

A helpful approach to responding to these questions includes the following:

- Read the entire stem and determine what the question is asking. Look for keywords such as “BEST,” “MOST,” “FIRST,” etc., and key terms that may indicate what domain or concept is being tested.
- Read all the options, and then read the stem again to see if you can eliminate any of the options based on your immediate understanding of the question.
- Re-read the remaining options and bring in any personal experience to determine which is the best answer to the question.

Another condition the candidate should consider when preparing for the exam is to recognize that information security is a global profession, and individual perceptions and experiences may not reflect the more global position or circumstance. Because the exam and CISM manuals are written for the international information security community, the candidate will be required to be somewhat flexible when reading a condition that may be contrary to the candidate's experience. It should be noted that CISM exam questions are written by experienced information security managers from around the world. Each question on the exam is reviewed by ISACA's CISM Exam Item Development Working Group, which consists of international members. This geographic representation ensures that all exam questions are understood equally well in every country and language.

Any suggestions to enhance the manual or questions related to the contents should be sent to *studymaterials@isaca.org*.

Page intentionally left blank

PRETEST

If you wish to take a pretest to determine strengths and weaknesses, the Sample Exam begins on page 417 and the pretest answer sheet begins on page 436. You can score your pretest with the Sample Exam Answer and Reference Key on page 440.

Page intentionally left blank

QUESTIONS, ANSWERS AND EXPLANATIONS BY DOMAIN

DOMAIN 1—INFORMATION SECURITY GOVERNANCE (17%)

1. Which of the following is the **MOST** effective way to ensure that noncompliance to information security standards is resolved?

   A. Periodic audits of noncompliant areas
   B. An ongoing vulnerability scanning program
   C. Annual security awareness training
   D. Regular reports to the audit committee

D is the correct answer.

Justification:

A. Periodic audits can be effective but only when combined with reporting.
B. Vulnerability scanning has little to do with noncompliance with standards.
C. Training can increase management's awareness regarding information security, but awareness training is generally not as compelling to management as having individual names highlighted on a compliance report.
D. Reporting noncompliance to the audit committee is the most effective way to have enforcement for concerned parties to take the proper action in order to comply.

2. Senior management commitment and support for information security can **BEST** be obtained through presentations that:

   A. use illustrative examples of successful attacks.
   B. explain the technical risk to the enterprise.
   C. evaluate the enterprise against good security practices.
   D. tie security risk to key business objectives.

D is the correct answer.

Justification:

A. Senior management may not be as interested in examples of successful attacks if they are not tied to the impact on business environment and objectives.
B. Senior management will not be as interested in technical risk to the enterprise if it is not tied to the impact on business environment and objectives.
C. Industry good practices may be important to senior management to the extent they are relevant to the enterprise and its business objectives; however, this is not the best method of gaining commitment and support for information security.
D. Tying security risk to key business objectives is the best option to obtain senior managers' commitment and support as they want to understand the justification for investing in security in relation to achieving key business objectives.

END OF PREVIEW