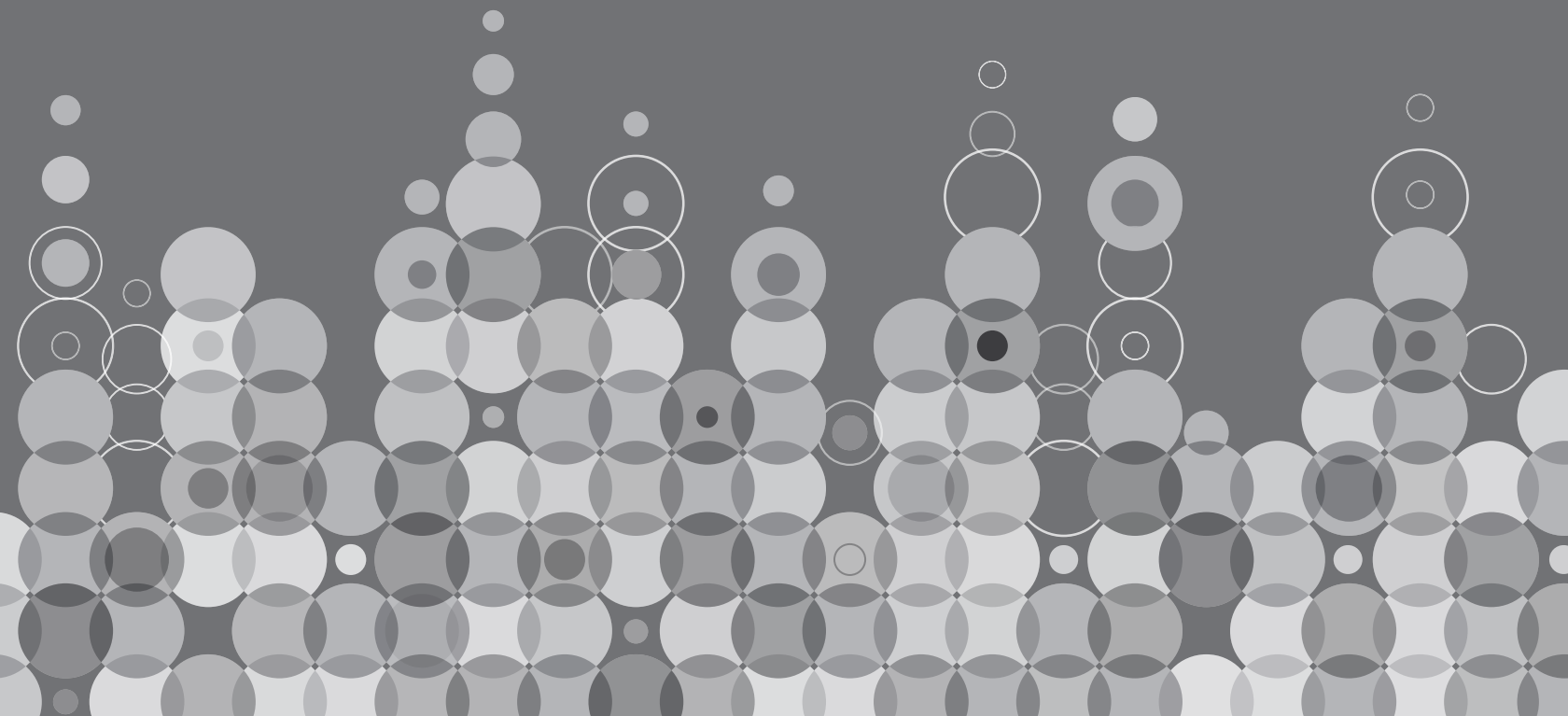
ISACA®
Trust in, and value from, information systems

15th Edition

CISM

Review Manual

CISM® Certified Information Security Manager®
An ISACA® Certification



ISACA®
ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

In addition, ISACA advances and validates business-critical 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™) credentials.

Disclaimer
ISACA has designed and created *CISM® Review Manual 15th 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 Working Group, 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.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN 978-1-60420-508-4
CISM® Review Manual 15th Edition
Printed in the United States of America

CISM REVIEW MANUAL 15TH EDITION

ISACA is pleased to offer the 15th edition of the *CISM® Review Manual.* The purpose of this manual is to provide CISM candidates with updated technical information and references to assist in the preparation and study for the Certified Information Security Manager exam.

The *CISM® Review Manual* is updated to keep pace with rapid changes in the management, design, oversight and assessment of information security. As with previous manuals, the 15th edition is the result of contributions from many qualified authorities who have generously volunteered their time and expertise. We respect and appreciate their contributions and feel certain their efforts will provide extensive educational value to CISM manual readers.

Your comments and suggestions regarding this manual are welcome. After taking the exam, please take a moment to complete the online questionnaire *(www.isaca.org/studyaidsevaluation*). Your observations will be invaluable for the preparation of the 16th edition of the *CISM® Review Manual*.

The self-assessment questions contained in this manual are designed to depict the type of questions typically found on the CISM exam and to provide further clarity to the content presented in this manual. The CISM exam is a practice-based exam. Simply reading the reference material in this manual will not properly prepare candidates for the exam. The self-assessment questions are included for guidance only. Scoring results do not indicate future individual exam success.

Certification has resulted in a positive impact on many careers. CISM is designed to provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective information security management and consulting. While the central focus of the CISM certification is information security management, all those in the IT profession with security experience will certainly find value in the CISM designation. ISACA wishes you success with the CISM exam.

ACKNOWLEDGMENTS

The 15th edition of the *CISM® Review Manual* is the result of the collective efforts of many volunteers. ISACA members from throughout the global information security management profession participated, generously offering their talent and expertise. This international team exhibited a spirit and selflessness that has become the hallmark of contributors to this manual. Their participation and insight are truly appreciated.

All of the ISACA members who participated in the review of the *CISM® Review Manual* deserve our thanks and gratitude.

Special thanks go to W. Krag Brotby, CISM, CGEIT, a senior security consultant from the Sacramento (California) Chapter, USA, who served as technical content project leader and editor.

Expert Reviewers
Michael Broady, CISM, CRISC, ACE, US Southern Command/Exeter Cooperation, USA
Mouhamed Diop, CISA, CISM, CGEIT, CRISC, Senegal
Sandeep Godbole, CISA, CISM, CGEIT, CEH, CISSP, Syntel, India
Mohamed Gohar, CISA, CISM, COBIT Foundation, CPDE, ISO 27001, 27034, 38500 and 24762 certified, ITIL Expert, PECB-CLPTP, PMP, Resilia Practitioner, TOGAF Practitioner, Itpreneurs, Global Knowledge, AUC, El-Khalij Institute or New Horizons and Egybyte, Egypt
Robert T. Hanson, CISA, CISM, CRISC, CRMA, Australian Government, Australia
Foster Henderson, CISM, CRISC, CISSP, USA
Kevin Henry, CISA, CISM, CRISC, CISSP, Canada
Abdus Sami Khan, CISA, CISM, CIA, SALE Advanced Co. Ltd., Saudi Arabia
Israel Rosales M., CISA, CISM, CRISC, CEH, CHFI, CISSP, COBIT 5, ISO 27001LA, ITIL, COSIM TI, Bolivia
Cory Missimore, CISM, USA
Juan Carlos Morales, CISA, CISM, CGEIT, CRISC, Guatemala
Balakrishnan Natarajan, CISM, Pivotal Software Inc., USA
S. Peter Nota, CISA, CISM, APMP, CISSP, MBCS, PCI-ISA, Premier Farnell plc, UK
Opeyemi Onifade, CISA, CISM, CGEIT, CISSP, COBIT Accredited Trainer, COBIT Certified Assessor, Afenoid Enterprise Limited, Nigeria
Vaibhav Patkar, CISA, CISM, CRISC, CGEIT, CISSP, India
Abdul Jaleel Puthenpurayil, CISM, United Arab Emirates
Ravikumar Ramachandran, CISA, CISM, CGEIT, CRISC, CAP, CEH, CFE, CHFI, CIA, CISSP-ISSAP, CIA, CIMA-Adv. Dip. MA, CRMA, ECSA, FCMA , PMP, SSCP, Hewlett-Packard India Sales Pvt. Ltd, India
James C. Samans, CISA, CISM, CRISC, CISSP-ISSEP, CPP, CIPT, CEH, PMP, XENSHA LLC, USA
Pavel Strongin, CISA, CISM, CPA, Charter Communications, USA
Darlene M. Tester, CISM, CISSP, Mystic Lake Hotel & Casino, USA
Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CCSP, CBCP, CDP, CISSP, ITIL v3, Veris Group, LLC, USA

ISACA has begun planning the 16th edition of the *CISM® Review Manual*. Volunteer participation drives the success of the manual. If you are interested in becoming a member of the select group of professionals involved in this global project, we want to hear from you. Please email us at *studymaterials@isaca.org.*

NEW—CISM JOB PRACTICE

BEGINNING IN 2017, 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 2017.

The primary focus of the job practice is 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 2017 job practice reflects the areas of study to be tested and is compared below to the previous job practice. The complete CISM job practice can be found at *www.isaca.org/cismjobpractice*.

Previous CISM Job Practice	New 2017 CISM Job Practice
Domain 1: Information Security Governance (24%)	**Domain 1: Information Security Governance (24%)**
Domain 2: Information Risk Management and Compliance (33%)	**Domain 2: Information Risk Management (30%)**
Domain 3: Information Security Program Development and Management (25%)	**Domain 3: Information Security Program Development and Management (27%)**
Domain 4: Information Security Incident Management (18%)	**Domain 4: Information Security Incident Management (19%)**

Page intentionally left blank

Table of Contents

About This Manual

Overview

The *CISM® Review Manual 15th Edition* is a reference guide designed to assist candidates in preparing for the CISM examination. **The manual is one source of preparation for the exam and should not be thought of as the only source nor viewed as a comprehensive collection of all the information and experience that are required to pass the exam.** No single publication offers such coverage and detail.

As candidates read through the manual and encounter topics that are new to them or ones in which they feel their knowledge and experience are limited, additional references should be sought. The examination will be composed of questions testing the candidate's technical and practical knowledge and his/her ability to apply the knowledge (based on experience) in given situations.

Organization of This Manual

The *CISM® Review Manual 15th Edition* is divided into four chapters covering the CISM domains tested on the exam in the percentages listed below:

Domain 1	Information Security Governance	24 percent
Domain 2	Information Risk Management	30 percent
Domain 3	Information Security Program Development and Management	27 percent
Domain 4	Information Security Incident Management	19 percent

Note: Each chapter defines the tasks that CISM candidates are expected to know how to do and includes a series of knowledge statements required to perform those tasks. These constitute the current practices for the information security manager. **The detailed CISM job practice can be viewed at *www.isaca.org/cismjobpractice*. The exam is based on these task and knowledge statements.**

The manual has been developed and organized to assist in the study of these areas. Exam candidates should evaluate their strengths, based on knowledge and experience, in each of these areas.

Format of This Manual

Each of the four chapters of the *CISM® Review Manual 15th Edition* is divided into two sections for focused study.

Section one includes:
- A definition of the domain
- Learning objectives for the domain as a practice area
- A listing of the task and knowledge statements for the domain
- A map of the relationship of each task to the knowledge statements for the domain
- A reference guide for the knowledge statements for the domain, including the relevant concepts and explanations
- References to specific content in section two for each knowledge statement
- Sample self-assessment questions and answers with explanations
- Suggested resources for further study of the domain

Section two includes:
- Reference material and content that supports the task and knowledge statements
- Definitions of terms most commonly found on the exam
- Learning activities to reinforce concepts and knowledge

Material included is pertinent for the CISM candidate's knowledge and/or understanding when preparing for the CISM certification exam.

The structure of the content includes numbering to identify the chapter where a topic is located and headings of the subsequent levels of topics addressed in the chapter (i.e., 2.1.1 The Importance of Risk Management is a subtopic of Risk Management Overview in chapter 2). Relevant content in a subtopic is bolded for specific attention.

Understanding the material is a barometer of the candidate's knowledge, strengths and weaknesses, and is an indication of areas in which the candidate needs to seek additional external reference sources. However, written material is not a substitute for experience. **CISM exam questions will test the candidate's practical application of this knowledge.**

Although every effort is made to address the majority of information that candidates are expected to know, not all examination questions are necessarily covered in the manual, and candidates will need to rely on professional experience to provide the best answer.

Throughout the manual, "association" refers to ISACA, formerly known as Information Systems Audit and Control Association, and "institute" or "ITGI®" refers to the IT Governance Institute®. Also, please note that the manual has been written using standard American English.

Note: The *CISM® Review Manual 15th Edition* is a living document. As technology advances and information security management practices evolve, the manual will be updated to reflect such changes. Further updates to this document before the date of the exam may be viewed at *www.isaca.org/studyaidupdates.*

Evaluation of This Manual

ISACA continuously monitors the swift and profound professional, technological and environmental advances affecting the information security management profession. Recognizing these rapid advances, the *CISM® Review Manual* is updated annually.

To assist ISACA in keeping abreast of these advances, please take a moment to evaluate the *CISM® Review Manual 15th Edition*. Such feedback is valuable to fully serve the profession and future CISM exam registrants.

To complete the evaluation on the web site, please go to *www.isaca.org/studyaidsevaluation.*

Thank you for your support and assistance.

Preparing for the CISM Exam

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

CISM Self-assessment

In order to effectively study for the CISM exam, you should first identify the job practice areas in which you are weak. A good starting point is the CISM self-assessment, available at http://*www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/CISM-Self-Assessment.aspx*

This 50-question sample exam is based upon the question distribution of the CISM exam and can provide you with a high-level evaluation of your areas of needs. When you complete the self-assessment, you will receive a summary of how you performed in each of the four job practice domains. You can use this summary to review the task and knowledge statements in the job practice and get an idea of where you should primarily focus your study efforts.

USING THE CISM REVIEW MANUAL

The *CISM Review Manual* is divided into four chapters, each corresponding with a domain in the CISM job practice. The content of the chapters is organized around the task statements for each chapter. While the Review Manual does not include every concept that could be tested on the CISM exam, it does cover a breadth of knowledge that provides a solid base for the exam candidate. **The manual is one source of preparation for the exam and should not be thought of as the only source nor viewed as a comprehensive collection of all the information and experience that are required to pass the exam.**

Manual Features

The *CISM Review Manual* includes several features to help you navigate the CISM job practice and enhance your learning and retention of the material.

Task Statement Reference Guide
The Task Statement Reference Guide maps the task statement in each domain to relevant sections in the Review Manual. This guide can be used in conjunction with other study materials, such as the *CISM Review Questions, Answers & Explanations Manual 9th Edition*, to help you easily find content related to the task statements you want to review.

Self-assessment Questions and Answers
The self-assessment questions at the end of section one of each chapter assist in understanding how a CISM question could be presented on the CISM exam and should not be used independently as a source of knowledge. Self-assessment questions should not be considered a measurement of the candidate's ability to answer questions correctly on the CISM exam for that area. The questions are intended to familiarize the candidate with question structure, and may or may not be similar to questions that will appear on the actual examination.

Suggested Resources for Further Study
As many of the concepts presented within the Review Manual are complex, you may find it useful to refer to external sources to supplement your understanding of these concepts. The suggested resources are references you can use to help to enhance your study efforts as they relate to each chapter.

In Practice
The In Practice questions are designed for you to further explore concepts from the Review Manual in your own practice. These questions are prompts that may require you to look into your organization's practices to reinforce the material presented in that specific session. For further exploration, consider interacting with colleagues on the ISACA forums or social media platforms.

Knowledge Checks
Knowledge Checks are activities designed to put the material from the Review Manual into practice. These include matching questions, scenarios, recall questions and other activities to further enhance your learning. Answers are provided at the end of each chapter, but it is suggested that you attempt to complete the Knowledge Check prior to referring to the answer key.

Case Studies
Case studies provide scenario-based learning that focuses on the concepts presented within each chapter. Each case study includes an information security management scenario related to each domain and questions related to the scenario. The purpose of these cases studies is to provide a real-world perspective on the content of each domain and how it relates to the CISM's practice.

Glossary
A glossary is included at the end of the manual and contains terms that apply to the material included in the chapters. Also included are terms that apply to related areas not specifically

discussed. The glossary is an extension of the text in the manual and can, therefore, be another indication of areas in which the candidate may need to seek additional references.

USING THE CISM REVIEW MANUAL WITH OTHER ISACA RESOURCES

The *CISM Review Manual* can be used in conjunction with other CISM exam preparation. These products are based on the CISM job practice, and referenced task and knowledge statements can be used to find related content within the *CISM Review Manual.* These resources include:

- *CISM Review Questions, Answers and Explanations Manual 9th Edition*
- CISM Review Questions, Answers and Explanations Database – 12 Month Subscription
- Chapter CISM Review Courses

ABOUT THE CISM REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS PRODUCTS

The *CISM® Review Questions, Answers & Explanations Manual 9th Edition* consists of 1,000 multiple-choice study questions, answers and explanations arranged in the domains of the current CISM job practice.

Another study aid that is available is the **CISM® Review Questions, Answers & Explanations Database – 12 Month Subscription.** The database consists of the 1,000 questions, answers and explanations included in the *CISM® Review Questions, Answers & Explanations Manual 9th Edition*. With this product, CISM candidates can quickly identify their strengths and weaknesses by taking random sample exams of varying length and breaking the results down by domain. Sample exams also can be chosen by domain, allowing for concentrated study, one domain at a time, and other sorting features such as the omission of previous correctly answered questions are available.

Questions in these products are representative of the types of questions that could appear on the exam and include explanations of the correct and incorrect answers. Questions are sorted by the CISM domains and as a sample test. These products are ideal for use in conjunction with the *CISM® Review Manual 15th Edition*. These products can be used as study sources throughout the study process or as part of a final review to determine where candidates may need additional study. It should be noted that these questions and suggested answers are provided as examples; they are not actual questions from the examination and may differ in content from those that actually appear on the exam.

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. As previously mentioned, 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 to answer them will go a long way toward answering them correctly. The best answer is 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 these questions includes the following:

- Read the entire stem and determine what the question is asking. Look for key words such as "BEST," "MOST," "FIRST," etc. and key terms that may indicate what domain or concept that is being tested.
- Read all of 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 in every country and language.

Note: When using the CISM review materials to prepare for the exam, it should be noted that they cover a broad spectrum of information security management issues. **Again, candidates should not assume that reading these manuals and answering review questions will fully prepare them for the examination.** Since actual exam questions often relate to practical experiences, candidates should refer to their own experiences and other reference sources, and draw upon the experiences of colleagues and others who have earned the CISM designation.

Page intentionally left blank

Chapter 1:

Information Security Governance

Section One: Overview

Section Two: Content

Section One: Overview

This chapter reviews the body of knowledge and associated tasks necessary to develop an information security governance structure aligned with organizational objectives.

DOMAIN DEFINITION

Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives.

LEARNING OBJECTIVES

The objective of this domain is to ensure that the CISM candidate has the knowledge necessary to:

- Understand the purpose of information security governance, what it consists of and how to accomplish it
- Understand the purpose of an information security strategy, its objectives, and the reasons and steps required to develop one
- Understand the meaning, content, creation and use of policies, standards, procedures and guidelines and how they relate to each other
- Develop business cases and gain commitment from senior leadership
- Define governance metrics requirements, selection and creation

CISM EXAM REFERENCE

This domain represents 24 percent of the CISM examination (approximately 36 questions).

TASK AND KNOWLEDGE STATEMENTS

TASK STATEMENTS

There are nine tasks within this domain that a CISM candidate must know how to perform:

T1.1 Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

T1.2 Establish and/or 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 guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

T1.5 Develop business cases to support investments in information security.

T1.6 Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.

T1.7 Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

T1.8 Define, communicate and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.

T1.9 Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

KNOWLEDGE STATEMENTS

The CISM candidate must have a good understanding of each of the areas delineated by the knowledge statements. These statements are the basis for the exam.

There are 19 knowledge statements within the information security governance domain:

K1.1 Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research)

K1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices

K1.3 Knowledge of available information security governance frameworks

K1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development

K1.5 Knowledge of the fundamental concepts of governance and how they relate to information security

K1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework

K1.7 Knowledge of methods to integrate information security governance into corporate governance

K1.8 Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development

K1.9 Knowledge of content in, and techniques to develop, business cases

K1.10 Knowledge of strategic budgetary planning and reporting methods

K1.11 Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy

K1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)

K1.13 Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security)

K1.14 Knowledge of roles and responsibilities of the information security manager
K1.15 Knowledge of organizational structures, lines of authority and escalation points
K1.16 Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users)
K1.17 Knowledge of processes to monitor performance of information security responsibilities
K1.18 Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
K1.19 Knowledge of methods to select, implement and interpret key information security metrics (e.g., key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])

RELATIONSHIP OF TASK TO KNOWLEDGE STATEMENTS

The task statements are what the CISM candidate is expected to know how to perform. The knowledge statements delineate each of the areas in which the CISM candidate must have a good understanding to perform the tasks. The task and knowledge statements are mapped, insofar as it is possible to do so. Note that although there is often overlap, each task statement will generally map to several knowledge statements.

Task and Knowledge Statements Mapping

Task Statement	Knowledge Statements
T1.1 Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.	K1.1 Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research) K1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices K1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development K1.10 Knowledge of strategic budgetary planning and reporting methods K1.11 Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy K1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)
T1.2 Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.	K1.3 Knowledge of available information security governance frameworks K1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development K1.5 Knowledge of the fundamental concepts of governance and how they relate to information security K1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework
T1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.	K1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices K1.3 Knowledge of available information security governance frameworks K1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development K1.5 Knowledge of the fundamental concepts of governance and how they relate to information security K1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework K1.7 Knowledge of methods to integrate information security governance into corporate governance
T1.4 Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.	K1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices K1.8 Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development
T1.5 Develop business cases to support investments in information security.	K1.9 Knowledge of content in, and techniques to develop, business cases K1.10 Knowledge of strategic budgetary planning and reporting methods K1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)

Task and Knowledge Statements Mapping *(cont.)*			
Task Statement		**Knowledge Statements**	
T1.6	Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.	K1.2 K1.7 K1.11	Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices Knowledge of methods to integrate information security governance into corporate governance Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy
T1.7	Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.	K1.12 K1.13	Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact) Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security)
T1.8	Define, communicate and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.	K1.15 K1.16 K1.17 K1.18	Knowledge of organizational structures, lines of authority and escalation points Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users) Knowledge of processes to monitor performance of information security responsibilities Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
T1.9	Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.	K1.10 K1.19	Knowledge of strategic budgetary planning and reporting methods Knowledge of methods to select, implement and interpret key information security metrics (e.g., key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])

TASK STATEMENT REFERENCE GUIDE

The following section contains the task statements a CISM candidate is expected to know how to accomplish mapped to and the areas in the review manual with information that supports the execution of the task. The references in the manual focus on the knowledge the information security manager must know to accomplish the tasks and successfully negotiate the exam.

Task Statement Reference Guide			
Task Statement		**Reference in Manual**	
T1.1	Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.	1.2 1.7 1.7.1 1.8 1.13	Effective Information Security Governance Information Security Strategy Overview Developing an Information Security Strategy Information Security Strategy Objectives Action Plan to Implement Strategy
T1.2	Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.	1.2.5 1.8.3	Business Model for Information Security The Desired State
T1.3	Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.	1.1 1.2.1 1.8.3 1.9 1.10	Information Security Governance Overview Business Goals and Objectives The Desired State Determining the Current State of Security Information Security Strategy Development
T1.4	Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.	1.3 1.11.1	Roles and Responsibilities Policies and Standards
T1.5	Develop business cases to support investments in information security.	1.4.2 3.10.8	Developing and Presenting the Business Case Business Case Development

Task Statement Reference Guide *(cont.)*			
Task Statement		**Reference in Manual**	
T1.6	Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.	1.5 1.12	Governance of Third-party Relationships Strategy Constraints
T1.7	Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.	1.4.2	Obtaining Senior Management Commitment
T1.8	Define, communicate and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.	1.3	Roles and Responsibilities
T1.9	Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.	1.6	Information Security Governance Metrics

SUGGESTED RESOURCES FOR FURTHER STUDY

Brotby, W. Krag, and IT Governance Institute; *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, ISACA, USA, 2006

Brotby, W. Krag, and IT Governance Institute; *Information Security Governance: Guidance for Information Security Managers,* ISACA, USA, 2008

Brotby, W. Krag; *Information Security Governance: A Practical Development and Implementation Approach*, Wiley & Sons, 2009

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 2013

International Organization for Standardization (ISO), *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements,* Switzerland, 2013

ISO, *ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls*, Switzerland, 2013

ISO, *ISO/IEC 27014:2013 Information technology—Security techniques—Governance of information security*, Switzerland, 2013

ISACA, *The Business Model for Information Security,* USA, 2010

ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*

ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/cobit*

ISACA, *COBIT® 5 for Information Security,* USA, 2012, *www.isaca.org/cobit*

National Institute of Standards and Technology (NIST), *NIST Special Publication 800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations*, USA, 2013

PricewaterhouseCoopers, *The Global State of Information Security Survey 2016, www.pwc.com/gx/en/consulting-services/information-security-survey*

Note: Publications in bold are stocked in the ISACA Bookstore.

SELF-ASSESSMENT QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every 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 a description problem 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. Many times a CISM examination question will require the candidate to choose the most likely or best answer.

In every case, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked, and how to study to gain knowledge of what will be tested, will go a long way toward answering them correctly.

1-1 A security strategy is important for an organization **PRIMARILY** because it:

A. provides a basis for determining the best logical security architecture for the organization.
B. provides the approach to achieving the outcomes management wants.
C. provides users guidance on how to operate securely in everyday tasks.
D. helps IS auditors ensure compliance.

1-2 Which of the following is the **MOST** important reason to provide effective communication about information security?

A. It makes information security more palatable to resistant employees.
B. It mitigates the weakest link in the information security landscape.
C. It informs business units about the information security strategy.
D. It helps the organization conform to regulatory information security requirements.

1-3 Which of the following approaches **BEST** helps the information security manager achieve compliance with various regulatory requirements?

A. Rely on corporate counsel to advise which regulations are the most relevant.
B. Stay current with all relevant regulations and request legal interpretation.
C. Involve all impacted departments and treat regulations as just another risk.
D. Ignore many of the regulations that have no penalties.

1-4 The **MOST** important consideration in developing security policies is that:

A. they are based on a threat profile.
B. they are complete and no detail is left out.
C. management signs off on them.
D. all employees read and understand them.

1-5 The **PRIMARY** security objective in creating good procedures is:

A. to make sure they work as intended.
B. that they are unambiguous and meet the standards.
C. that they are written in plain language and widely distributed.
D. that compliance can be monitored.

1-6 Which of the following **MOST** helps ensure that assignment of roles and responsibilities is effective?

A. Senior management is in support of the assignments.
B. The assignments are consistent with existing proficiencies.
C. The assignments are mapped to required skills.
D. The assignments are given on a voluntary basis.

1-7 Which of the following benefits is the **MOST** important to an organization with effective information security governance?

A. Maintaining appropriate regulatory compliance
B. Ensuring disruptions are within acceptable levels
C. Prioritizing allocation of remedial resources
D. Maximizing return on security investments

1-8 From an information security manager's perspective, the **MOST** important factors regarding data retention are:

A. business and regulatory requirements.
B. document integrity and destruction.
C. media availability and storage.
D. data confidentiality and encryption.

1-9 Which role is in the **BEST** position to review and confirm the appropriateness of a user access list?

A. Data owner
B. Information security manager
C. Domain administrator
D. Business manager

1-10 In implementing information security governance, the information security manager is **PRIMARILY** responsible for:

A. developing the security strategy.
B. reviewing the security strategy.
C. communicating the security strategy.
D. approving the security strategy.

ANSWERS TO SELF-ASSESSMENT QUESTIONS

1-1 A. Policies have to be developed to support the security strategy, and an architecture can only be developed after policies are completed (i.e., the security strategy is not the basis for architecture; policies are).
B. A security strategy will define the approach to achieving the security program outcomes management wants. It should also be a statement of how security aligns with and supports business objectives, and it provides the basis for good security governance.
C. A security strategy may include requirements for users to operate securely, but it does not address how that is to be accomplished.
D. IS auditors do not determine compliance based on strategy, but rather on elements such as standards and control objectives.

1-2 A. Effective communication may assist in making information security more palatable, but that is not the most important aspect.
B. Security failures are, in the majority of instances, directly attributable to lack of awareness or failure of employees to follow policies or procedures. Communication is important to ensure continued awareness of security policies and procedures among staff and business partners.
C. Effective communication will allow business units to be informed about various aspects of information security, including the strategy, but it is not the most important aspect.
D. Effective communication will assist in achieving compliance because it is unlikely that employees will be compliant with regulations unless they are informed about them. However, it is not the most important consideration.

1-3 A. Corporate counsel is generally involved primarily with stock issues and the associated filings required by regulators and with contract matters. It is unlikely that legal staff will be current on information security regulations and legal requirements.
B. While it can be useful to stay abreast of all current and emerging regulations, it is, as a practical matter, nearly impossible, especially for a multinational company.
C. Departments such as human resources, finance and legal are most often subject to new regulations and, therefore, must be involved in determining how best to meet the existing and emerging requirements and, typically, would be most aware of these regulations. Treating regulations as another risk puts them in the proper perspective, and the mechanisms to deal with them should already exist. The fact that there are so many regulations makes it unlikely that they can all be specifically addressed efficiently. Many do not currently have significant consequences and, in fact, may be addressed by compliance with other regulations. The most relevant response to regulatory requirements is to determine potential impact to the organization just as must be done with any other risk.
D. Even if certain regulations have few or no penalties, ignoring them without consideration for other potential impacts (e.g., reputational damage) and whether they might be relevant to the organization is not generally a prudent approach.

1-4 **A. The basis for developing relevant security policies is addressing viable threats to the organization, prioritized by the likelihood of occurrence and their potential impact on the business. The strictest policies apply to the areas of greatest business value. This ensures that protection proportionality is maintained.**
B. Policies are a statement of management's intent and direction at a high level and provide little, if any, detail.
C. While the policies are being developed, management would not be asked to sign them until they have been completed.
D. Employees would not be reading and understanding the policies while they are being developed.

1-5 A. While it is important to make sure that procedures work as intended, the fact that they do not may not be a security issue.
B. All of the answers are important, but the first criterion must be to ensure that there is no ambiguity in the procedures and that, from a security perspective, they meet the applicable standards and, therefore, comply with policy.
C. Of importance, but not as critical, is that procedures are clearly written and that they are provided to all staff as needed.
D. Compliance is important, but it is essential that it is compliant with a correct procedure.

1-6 A. Senior management support is always important, but it is not of as significant importance to the effectiveness of employee activities.
B. The level of effectiveness of employees will be determined by their existing knowledge and capabilities—in other words, their proficiencies.
C. Mapping roles to the tasks that are required can be useful but it is no guarantee that people can perform the required tasks.
D. While employees are more likely to be enthusiastic about a job they have volunteered for, it is not a requirement for them to be effective.

1-7 A. Maintaining appropriate regulatory compliance is a useful, but subordinate, outcome.
B. The bottom line of security efforts is to ensure that business can continue to operate with an acceptable level of disruption that does not unduly constrain revenue-producing activities.
C. Prioritizing allocation of remedial resources is a useful, but subordinate, outcome.
D. Maximizing return on security investments is a useful, but subordinate, outcome.

1-8 **A. Business and regulatory requirements are the driving factors for data retention.**
B. Integrity is a key factor for information security; however, business and regulatory requirements are the driving factors for data retention.
C. Availability is a key factor for information security; however, business and regulatory requirements are the driving factors for data retention.
D. Confidentiality is a key factor for information security; however, business and regulatory requirements are the driving factors for data retention.

1-9 **A. The data owner is responsible for periodic reconfirmation of the access lists for systems he/she owns.**
B. The information security manager is in charge of the coordination of the user access list reviews but he/she does not have any responsibility for data access.
C. The domain administrator may technically provide the access, but he/she does not approve it.
D. The business manager is incorrect because the business manager may not be the data owner.

1-10 **A. The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners and senior management.**
B. The information security strategy is the responsibility of a steering committee and/or senior management.
C. The information security manager is not necessarily responsible for communicating the security strategy.
D. Final approval of the information security strategy must be made by senior management.