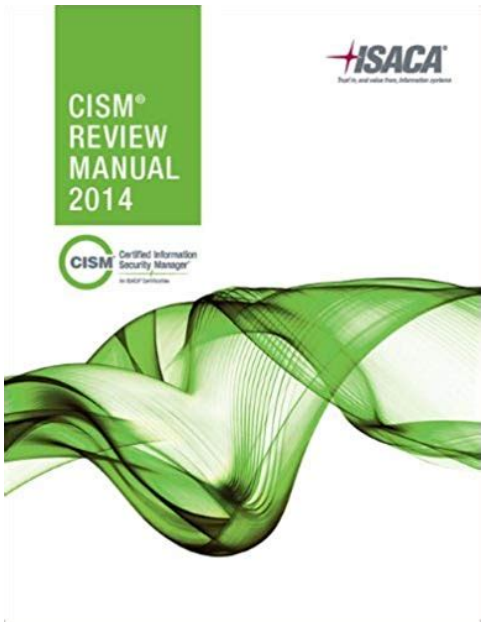
Download Cism Review Manual 2011



File Name: Download Cism Review Manual 2011.pdf
Size: 4299 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 11 May 2019, 19:47 PM
Rating: 4.6/5 from 588 votes.

Status: AVAILABLE

Last checked: 10 Minutes ago!

In order to read or download Download Cism Review Manual 2011 ebook, you need to create a FREE account.

Download Now!

eBook includes PDF, ePub and Kindle version

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with Download Cism Review Manual 2011 . To get started finding Download Cism Review Manual 2011 , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

Book Descriptions:

Download Cism Review Manual 2011

Used GoodCustomer service is our top priority!Please try again.Please try again.Please try again. The manual has been continually enhanced over the past six editions and is a current, comprehensive, peerreviewed information security management global resource. The 2012 edition assists helps candidates study and understand essential concepts in the following job practice areas Information Security Governance Information Risk Management and Compliance Information Security Program Development and Management Information Security Incident Management The CISM Review Manual 2012 retains the easytonavigate format first introduced in 2010. Each of the books four chapters has been divided into two sections for focused study. The first section contains the definitions and objectives for the four areas, with the corresponding tasks and knowledge statements that are tested on the exam. Section one of each chapter is an overview that provides Definitions for the four areas Objectives for each area Descriptions of the tasks A map of the relationship of each task to the knowledge statement A reference guide for the knowledge statements, including the relevant concepts and explanations References to specific content in section two for each knowledge statement Sample practice questions and explanations of the answers Suggested resources for further study Section two of each chapter consists of reference material and content that support the knowledge statements. Also included are definitions of terms most commonly found on the exam. This manual is effective as a standalone document for individual study and as a guide or reference for study groups and chapters conducting local review courses. It is also a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.http://www.oma.org.tw/public_html/pics/98-ford-focus-manual.xml

- **download cism review manual 2011, download cism review manual 2011 pdf, download cism review manual 2011 free, download cism review manual 2011 version.**

Then you can start reading Kindle books on your smartphone, tablet, or computer no Kindle device required. Register a free business account To calculate the overall star rating and percentage breakdown by star, we don’t use a simple average. Instead, our system considers things like how recent a review is and if the reviewer bought the item on Amazon. It also analyzes reviews to verify trustworthiness. Please try again later. Anand Joseph 4.0 out of 5 stars To look up a term in the index, many words are referenced on multiple pages but are only mentioned in passing without a specific explanation of the term. If I could get my money back, I would.I have worked in IT and information security but this book was a great help in preparing for the exam which I passed. Note This book CISM Review Manual 2015 has 24 ratings and 4 reviews. Jussi said Gives a good knowledge of CISM certification. Helps a lot if u want to certify yourself To improve the usefulness of future manuals, the ISACA Board of Directors would appreciate you taking a moment to evaluate the CISM Review Manual. Author, Isaca. Publisher, Information Systems Audit and Control Association, 2017. ISBN, 1604207027 Missouri annual registration report, Irs form payment over 10,000.00, Weather report oakland ca, Scorpion bug guide, Where to get irs form 1040. Reload to refresh your session. Reload to refresh your session. These questions are \nrepresentative of ISM questions, although they are not actual test items. They are provided to \nassist the CISM candidate in understanding the material in the CISM Review Manual 2011 and to \ndepict the type of question format typically found on the C1SM exam.\n \n Sample Exam\nA random sample exam of 200 of the questions is also provided in this manual. Candidates are \nurged to use this sample test and the answer sheets provided to simulate an actual exam. Many \ncandidates use this exam as a pretest to

determine strengths or weaknesses, or as a final exam.http://antropolog.ru/userfiles/file/98-ford-mustang-owners-manual.xml

\nSample exam answer sheets have been provided for both uses. These sample exam questions have been crossreferenced to \nthe questions, answers and explanations by area, so it is convenient to refer to the explanations \nof the correct answers. As\nyou use this publication to prepare for the exam, please note that it covers a broad spectrum of\ninformation security management issues. Do not assume that reading and working the questions\nin this manual will fully prepare you for the exam. These additional references are an\nexcellent source of further detailed information and clarification. As\npreviously mentioned, all questions are presented in a multiple choice format and are designed\nfor one best answer.\n \n The candidate is cautioned to read each question carefully. Many times a CISM exam question \nwill require the candidate to choose the appropriate answer that is MOST likely or BEST, or, the \ncandidate may be asked to choose a practice or procedure that would be performed FIRST \n \n INTRODUCTION \n\n \n related to the other answers. In every case, the candidate is required to read the question \ncarefully, eliminate known wrong answers and then make the best choice possible. Knowing that \nthese types of questions are asked and how to study to answer them will go a long way toward \nanswering them correctly.\n \n Each CISM question has a stem question and four options answer choices. The candidate is \nasked to choose the correct or best answer from the options. The stem may be in the form of a \nquestion or incomplete statement. In some instances, a scenario or description also may be \nincluded.

These questions normally include a description of a situation and require the candidate\nto answer two or more questions based on the information provided\n \n Another condition the candidate should consider when preparing for the exam is to recognize \nthat information security is a global profession, and individual perceptions and experiences may \nnot reflect the more global position or circumstance. Each question on the exam is reviewed by ISACAs CISM Test \nEnhancement Committee and CISM Certification Committee, which consist of international \nmembers. This geographic representation ensures that all test questions are understood equally \nin every country and language.\n \n Note ISACA review manuals are living documents. As technology advances, ISACA \nmanuals will be updated to reflect such advances. The primary focus of the job practice is on the current \ntasks performed and the knowledge used by CISMs. By gathering evidence of the current work \npractice of CISMs, ISACA is able to ensure that the CISM program continues to meet the high \nstandards for the certification of professionals throughout the world.\n \n All review manual and exam content has been enhanced to cover the current practices for the \ninformation security manager. Analyze the current business strategy\nC. Perform a business impact analysis\nD. Assess the current levels of security awareness\n \n B Prior to assessing technical vulnerabilities or levels of security awareness, an information \nsecurity manager needs to gain an understanding of the current business strategy and \ndirection. A business impact analysis should be performed prior to developing a business \ncontinuity plan, but this would not be an appropriate first step in developing an \ninformation security strategy because it focuses on availability.\n \n S12 Senior management commitment and support for information security can BEST be \nobtained through presentations that\n \n A.

http://www.bosport.be/newsletter/defy-gemini-manual

use illustrative examples of successful attacks.\nB. explain the technical risks to the organization.\nC. evaluate the organization against best security practices.\nD. tie security risks to key business objectives.\n \n D Senior management seeks to understand the business justification for investing in security.\nThis can best be accomplished by tying security to key business objectives. Senior \nmanagement will not be as interested in technical risks or examples of successful attacks \nif they are not tied to the impact on business environment and objectives. Industry best \npractices are important to senior management but, again, senior management will give \nthem the right level

of importance when they are presented in terms of key business \nobjectives.\n \n S13 The MOST appropriate role for senior management in supporting information security is the\n \n A. evaluation of vendors offering security products.\nB. assessment of risks to the organization.\nC. approval of policy statements and funding.\nD. monitoring adherence to regulatory requirements.\n \n C Since the members of senior management are ultimately responsible for information \nsecurity, they are the ultimate decision makers in terms of governance and direction. They\nare responsible for approval of major policy statements and requests to fund the \ninformation security practice. Evaluation of vendors, assessment of risks and monitoring \ncompliance with regulatory requirements are daytoday responsibilities of the information \nsecurity manager; in some organizations, business management is involved in these other \nactivities, though their primary role is direction and governance.\n \n S14 Which of the following would BEST ensure the success of information security governance \nwithin an organization\n \n A. Steering committees approve security projects\nB. Security policy training provided to all managers\nC. Security training available to all employees on the intranet\nD.

Steering committees enforce compliance with laws and regulations\n \n A The existence of a steering committee that approves all security projects would be an \nindication of the existence of a good governance program. Compliance with laws and \nregulations is part of the responsibility of the steering committee but it is not a full answer.\nAwareness training is important at all levels in any medium, and also an indicator of good \n\n \n governance. However, it must be guided and approved as a security project by the \nsteering committee.\n \n S15 Information security governance is PRIMARILY driven by\nA.Technology \nconstraints, regulatory requirements and litigation potential are all important factors, but \nthey are necessarily in line with the business strategy.\n \n S16 Which of the following represents the MAJOR focus of privacy regulations\nA. Unrestricted data mining\nB. Identity theft\nC. Human rights protection D.\nD. Identifiable personal data\n \n D Protection of identifiable personal data is the major focus of recent privacy regulations such\nas the Health Insurance Portability and Accountability Act HIPAA. Data mining is an \naccepted tool for ad hoc reporting; it could pose a threat to privacy only if it violates \nregulator provisions. Identity theft is a potential consequence of privacy violations but not\nthe main focus of many regulations. Human rights addresses privacy issues but is not the \nmain focus of regulations.\n \n S17 Investments in information security technologies should be based on\nA.Demonstrated value takes precedence over the current business climate \nbecause it is ever changing. Basing decisions on audit recommendations would be reactive\nin nature and might not address the key business needs comprehensively. Vulnerability \nassessments are useful, but they do not determine whether the cost is justified.\n \n S18 Retention of business records should PRIMARILY be based on\nA.

Storage capacity and longevity are important but secondary \nissues. Business case and value analysis would be secondary to complying with legal and \nregulatory requirements.\n \n S19 Which of the following is characteristic of centralized information security management\nA. More expensive to administer\nB. Better adherence to policies\nC. More aligned with business unit needs\nD. Faster turnaround of requests\n \n B Centralization of information security management results in greater uniformity and better \nadherence to security policies. It is generally less expensive to administer due to the \n\n \n economics of scale. However, turnaround can be slower due to the lack of alignment with \nbusiness units.\n \n S110 Successful implementation of information security governance will FIRST require\nA.Security procedures will necessitate specialized teams such as the computer \nincident response and management group as well as specialized tools such as the security \nmechanisms that comprise the security architecture. Security awareness will promote the \npolicies, procedures and appropriate use of the security mechanisms.\n \n Sl11 Which of the following individuals would be in the BEST position to sponsor the \ncreation of an information security steering group\n \n A. Information security manager\nB.

Chief operating officer COO\nC. Internal auditor\nD. Legal counsel\n \n B The chief operating officer COO is highlyplaced within an organization and has the most \nknowledge of business operations and objectives. The chief internal auditor and chief legal\ncounsel are appropriate members of such a steering group. However, sponsoring the \ncreation of the steering committee should be initiated by someone versed in the strategy \nand direction of the business. Since a security manager is looking to this group for \ndirection, they are not in the best position to oversee formation of this group.\n \n S112 The MOST important component of a privacy policy is\nA.

They do not necessarily address warranties, liabilities\nor geographic coverage, which are more specific.\n \n S113 The cost of implementing a security control should not exceed the\nA.A security mechanism may cost more than this amount or the cost of\na single incident and still be considered cost effective. Opportunity costs relate to revenue\nlost by forgoing the acquisition of an item or the making of a business decision.\n \n S1I4 When a security standard conflicts with a business objective, the situation should be \nresolved by\n \n A. changing the security standard.\nB. changing the business objective.\nC. performing a risk analysis. \n\n \n D. authorizing a risk acceptance.\n \n C Conflicts of this type should be based on a risk analysis of the costs and benefits of \nallowing or disallowing an exception to the standard. This document defines how components are secured and the \nsecurity services that should be in place. A strategy is a broad, highlevel document. A \nguideline is advisory in nature, while a security model shows the relationships between \ncomponents.\n \n S116 Which of the following is MOST appropriate for inclusion in an information security \nstrategy\nA. Business controls designated as key controls\nB. Security processes, methods, tools and techniques\nC. Firewall rule sets, network defaults and intrusion detection system IDS settings\nD. Budget estimates to acquire specific security tools\n \n B A set of security objectives, processes, methods, tools and techniques together constitute \na security strategy. Although IT and business governance are intertwined, business controls\nmay not be included in a security strategy. Budgets will generally not be included in an \ninformation security strategy. Additionally, until information security strategy is formulated \nand implemented, specific tools will not be identified and specific cost estimates will not be\navailable.

Firewall rule sets, network defaults and intrusion detection system IDS settings \nare technical details subject to periodic change, and are not appropriate content for a \nstrategy document.\n \n S117 Senior management commitment and support for information security will BEST be \nattained by an information security manager by emphasizing\n \n A. organizational risk.\nB. organization wide metrics.\nC. security needs.\nD. the responsibilities of organizational units.\n \n A Information security exists to help the organization meet its objectives. The information \nsecurity manager should identify information security needs based on organizational \nneeds. Organizational or business risk should always take precedence. Involving each \norganizational unit in information security and establishing metrics to measure success will\nbe viewed favorably by senior management after the overall organizational risk is \nidentified.\n \n S118 Which of the following roles would represent a conflict of interest for an information \nsecurity manager\nA. Evaluation of third parties requesting connectivity\nB. Assessment of the adequacy of disaster recovery plans \nC. Final approval of information security policies\nD. Monitoring adherence to physical security controls \n\n \n C Since management is ultimately responsible for information security, it should approve \ninformation security policy statements; the information security manager should not have \nfinal approval. Evaluation of third parties requesting access, assessment of disaster \nrecovery plans and monitoring of compliance with physical security controls are acceptable\npractices and do not present any conflicts of interest.\n \n S119 Which of the following situations must be corrected FIRST to ensure successful \ninformation security governance within an organization\n \n A. The information security department has difficulty filling vacancies.\nB. The chief information officer CIO approves security policy changes.\nC.

The information security oversight committee only meets quarterly.\nD. The data center manager has final signoff on all security projects.\n \n D A steering committee should be in place to approve all security projects. The fact that the \ndata center manager has final signoff for all security projects indicates that a steering \ncommittee is not being used and that information security is relegated to a subordinate \nplace in the organization. This would indicate a failure of information security governance. \nIt is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it\nmay be desirable to have the chief information officer CIO approve the security policy due\nto the size of the organization and frequency of updates. Difficulty in filling vacancies is not\nuncommon due to the shortage of good, qualified information security professionals.\n \n S120 Which of the following requirements would have the lowest level of priority in information \nsecurity\nA. Technical\nB. Regulatory\nC. Privacy\nD. Business\n \n A Information security priorities may, at times, override technical specifications, which then \nmust be rewritten to conform to minimum security standards. Regulatory and privacy \nrequirements are governmentmandated and, therefore, not subject to override. The needs\nof the business should always take precedence in deciding information security priorities.\n \n S121 When an organization hires a new information security manager, which of the following \ngoals should this individual pursue FIRST \n \n A. Develop a security architecture\nB. Establish good communication with steering committee members\nC. Assemble an experienced staff\nD. Benchmark peer organizations\n \n B New information security managers should seek to build rapport and establish lines of \ncommunication with senior management to enlist their support.

Benchmarking peer \norganizations is beneficial to better understand industry best practices, but it is secondary \nto obtaining senior management support. Similarly, developing a security architecture and \nassembling an experienced staff are objectives that can be obtained later.\n \n S122 It is MOST important that information security architecture be aligned with which of the \nfollowing\n \n A. Industry best practices\nB. Information technology plans\nC. Information security best practices\nD. Business objectives and goals \n\n \n D Information security architecture should always be properly aligned with business goals \nand objectives. Alignment with IT plans or industry and security best practices is secondary\nby comparison.\n \n S123 Which of the following is MOST likely to be discretionary\nA. Policies\nB. Procedures\nC. Guidelines\nD. Standards\n \n C Policies define security goals and expectations for an organization. These are defined in \nmore specific terms within standards and procedures. Standards establish what is to be \ndone while procedures describe how it is to be done. Guidelines provide recommendations \nthat business management must consider in developing practices within their areas of \ncontrol; as such, they are discretionary.\n \n S124 Security technologies should be selected PRIMARILY on the basis of their\nA.Investments in security \ntechnologies should be based on their overall value in relation to their cost; the value can \nbe demonstrated in terms of risk mitigation. This should take precedence over whether \nthey use new or exotic technologies or how they are evaluated in trade publications.\n \n S125 Which of the following are seldom changed in response to technological changes\n \n A. Standards\nB. Procedures\nC. Policies \nD. Guidelines\n \n C Policies are highlevel statements of objectives. Because of their highlevel nature and \nstatement of broad operating principles, they are less subject to periodic change.

Security \nstandards and procedures as well as guidelines must be revised and updated based on the \nimpact of technology changes.\n \n S126 The MOST important factor in planning for the longterm retention of electronically \nstored business records is to take into account potential changes in\n \n A. storage capacity and shelf life.\nB. regulatory and legal requirements.\nC. business strategy and direction.\nD. application systems and media.\n \n D Longterm retention of business records may be severely impacted by changes in \napplication systems and media. For example, data stored in nonstandard formats that can \nonly be read and interpreted by previously decommissioned applications may be difficult, if\nnot impossible, to recover. Business strategy and direction do not

generally apply, nor do \nlegal and regulatory requirements. Storage capacity and shelf life are important but \nsecondary issues. \n\n \n S127 Which of the following is characteristic of decentralized information security \nmanagement across a geographically dispersed organization\n \n A. More uniformity in quality of service\nB. Better alignment to business unit needs\nD. More savings in total operating costs\n \n C Decentralization of information security management generally results in better alignment \nto business unit needs. It is generally more expensive to administer due to the lack of \neconomies of scale. Uniformity in quality of service tends to vary from unit to unit.\n \n S128 Which of the following is the MOST appropriate position to sponsor the design and \nimplementation of a new security infrastructure in a large global enterprise\n \n A. Chief security officer CSO\nB. Chief privacy officer CPO\nD. Chief legal counsel CLC\n \n B The chief operating officer COO is most knowledgeable of business operations and \nobjectives.

The chief privacy officer CPO and the chief legal counsel CLC may not have \nthe knowledge of the day today business operations to ensure proper guidance, although \nthey have the same influence within the organization as the COO. Although the chief \nsecurity officer CSO is knowledgeable of what is needed, the sponsor for this task should \nbe someone with farreaching influence across the organization.\n \n S129 Which of the following would be the MOST important goal of an information security \ngovernance program\n \n A. Review of internal control mechanisms\nB. Effective involvement in business decision making\nC. Total elimination of risk factors\nD. Ensuring trust in data\n \n D The development of trust in the integrity of information among stakeholders should be the \nprimary goal of information security governance. Review of internal control mechanisms \nrelates more to auditing, while the total elimination of risk factors is not practical or \npossible. Proactive involvement in business decision making implies that security needs \ndictate business needs when, in fact, just the opposite is true. Involvement in decision \nmaking is important only to ensure business data integrity so that data can be trusted.\n \n S130 Relationships among security technologies are BEST defined through which of the \nfollowing\nA. Security metrics\nB. Network topology\nC. Security architecture\nD. Process improvement models\n \n C Security architecture explains the use and relationships of security mechanisms. Security \nmetrics measure improvement within the security practice but do not explain the use and \nrelationships of security technologies. Process improvement models and network topology \ndiagrams also do not describe the use and relationships of these technologies.\n \n S131 A business unit intends to deploy a new technology in a manner that places it in violation \nof existing information security standards.

What immediate action should an information \nsecurity manager take \n\n \n A. Enforce the existing security standard\nB. Change the standard to permit the deployment\nC. Perform a risk analysis to quantify the risk\nD. Perform research to propose use of a better technology\n \n C Resolving conflicts of this type should be based on a sound risk analysis of the costs and \nbenefits of allowing or disallowing an exception to the standard. A blanket decision should \nnever be given without conducting such an analysis. Enforcing existing standards is a good \npractice; however, standards need to be continuously examined in light of new \ntechnologies and the risks they present. Standards should not be changed without an \nappropriate risk assessment.\n \n S132 Acceptable levels of information security risk should be determined by\nA.Legal counsel, the \nexternal auditors and security management are not in a position to make such a decision.\n \n S133 The PRIMARY goal in developing an information security strategy is to\nA.Establishing \nmetrics and measuring performance, meeting legal and regulatory requirements, and \neducating business process owners are all subordinate to this overall goal.\n \n S134 Senior management commitment and support for information security can BEST be \nenhanced through\n \n A. a formal security policy sponsored by the chief executive officer CEO.\nB. regular security awareness training for employees.\nC. periodic review of alignment with business management goals.\nD. senior management signoff on the information security strategy.\n \n C Ensuring that security activities continue to be aligned and support business goals is \ncritical to obtaining their support.

Although having the chief executive officer CEO signoff \non the security policy and senior management signoff on the security strategy makes for \ngood visibility and demonstrates good tone at the top, it is a onetime discrete event that \nmay be quickly forgotten by senior management. Security awareness training for \nemployees will not have as much effect on senior management commitment.\n \n S135 When identifying legal and regulatory issues affecting information security, which of the \nfollowing would represent the BEST approach to developing information security policies\nA. Create separate policies to address each regulation\nB. Develop policies that meet all mandated requirements\nC. Incorporate policy statements provided by regulators\nD. Develop a compliance risk assessment\n \n B It will be much more efficient to craft all relevant requirements into policies than to create \nseparate versions. Using statements provided by regulators will not capture all of the \nrequirements mandated by different regulators. A compliance risk assessment is an \n\n \n important tool to verify that procedures ensure compliance once the policies have been \nestablished.\n \n S136 Which of the following MOST commonly falls within the scope of an information \nsecurity governance steering committee\n \n A. Interviewing candidates for information security specialist positions\nB. Developing content for security awareness programs\nC. Prioritizing information security initiatives\nD. Approving access to critical financial systems\n \n C Prioritizing information security initiatives is the only appropriate item. The interviewing of \nspecialists should be performed by the information security manager, while the developing \nof program content should be performed by the information security staff. Approving \naccess to critical financial systems is the responsibility of individual system data owners.