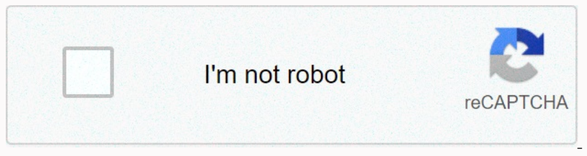

Continue

Crisc exam prep course session 2 pdf

You read free preview pages from 7 to 9 not displayed in this preview. You read free preview pages from 13 to 23 not displayed in this preview. You read free preview pages from 30 to 40 not displayed in this preview. Pages 44 to 49 free preview pages are not displayed in this view. You read free preview pages from 53 to 54 not displayed in this view. You read free preview pages from 58 to 68 not displayed in this preview. CRISC EXAM PREP COURSE: SESSION 3 2 Copyright 2016 ISACA. All rights reserved ID: 12355 Copyright of Work Practice 2016 ISACA. All rights reserved ID: 12355 DOMAIN 3 RISK RESPONSE AND MITIGATION 4 Copyright 2016 ISACA. All rights reserved ID: 12355 Area 3 Identify risk response options and evaluate their effectiveness and effectiveness to manage risks based on business goals. Domain 3 focuses on helping management to make decisions about the right way to respond to risks and address it in a corporate environment. 5 Copyright 2016 ISACA. All rights reserved ID: 12355 Learning objectives The aim of this area is to ensure that the CRISC candidate has the necessary knowledge: to list the various risk response options. Define the various parameters for risk response selection Please explain how residual risks are associated with inherent risks, appetite for risk and risk tolerance. When determining the risk response, discuss the need for a cost-benefit analysis. Develop a risk action plan. Explain the principles of risk ownership. Leverage understanding of the system development life cycle (SDLC) process to implement IS control efficiently and efficiently. Understand the need for control supervision. 6 Copyright 2016 ISACA. All rights reserved ID: 12355 The CRISC Exam Domain 3 accounts for 23% of questions on the CRISC exam (approximately 35 questions). Area 3 covers seven tasks related to the IT risk response. 7 Copyright 2016 ISACA. All rights reserved ID: 12355 Domain Tasks 3.1 Consult risk owners to select and combine recommended risk responses with business goals and enable informed risk solutions. 3.2 Consult or assist risk owners on the development of risk action plans to ensure that the plans include key elements (e.g. response, costs, target date). 3.3 Consult on the development, implementation or adjustment of mitigating controls to ensure that risks are managed to an acceptable level. 3.4 Ensure that control ownership is assigned to establish clear lines of accountability. 3.5 Assist control owners in developing control procedures and documents to effectively and effectively control enforcement. 3.6 Update the risk register to reflect risk changes and management's risk response. 3.7 Confirm that the risk response has been carried out in accordance with the risk action plans. 8 Copyright 2016 ISACA. All rights reserved ID: 12355 Task 3.1 with risk owners to choose and match the recommended risk response with business goals and enable informed risk solutions. 9 Copyright 2016 ISACA. All rights reserved ID: 12355 How to Task 3.1 relates to each of these statements of knowledge? Task Knowledge Statements Knowledge Statement Link 16. Organisational assets and business processes, including corporate risk management (ERM) Each asset shall have a defined risk owner who is consulted on the results of valuation and monitoring. The owner will help recommend answers that help you achieve your business goals. 17. Organisational policies and standards Should be subject to all organisational policies and standards adopted. Owners are responsible for ensuring that this policy reflects current business objectives. 27. Risk response options (i.e. accept, mitigate, avoid, transfer) and selection criteria The risk owner will consider business objectives to determine whether to assume, mitigate, avoid or transfer risks. 10 Copyright 2016 ISACA. All rights reserved ID: 12355 Who is responsible? Corporate governance, rather than an IT risk specialist, is ultimately responsible for risk control. This means that management is subject to the following responsibilities: maintaining awareness of the drivers of risk management By assessing and responding to the recommendations contained in the Risk Assessment Report The best risk response, the development of a response action plan and implementation strategy Senior management support for risk management and the control it needs should be visible and active. 11 Copyright 2016 ISACA. All rights reserved ID: 12355 Responsible practice THE IT risk specialist must consider risks and controls not only from the point of view of the IT department. Also need to take into account: Other enterprise divisions Business partners BUSINESS processes, supported by IT systems The best way to achieve a perspective that allows risk management to align with business goals is to communicate with senior management. Important objectives of this Communication: understanding management appetite for risk Learning about changes in the company's strategy New technologies Management Communications and Communication Infrastructure Development 12 Copyright 2016 ISACA. All rights reserved ID: 12355 The purpose of risk response is to reconcile the risk with the identified risk appetite of the undertaking. There are four generally accepted risk response or treatment categories. Risk Treatment 13 Copyright 2016 ISACA. All rights reserved ID: 12355 Risk acceptance To take risks, management must make a decision to allow or assume risks without attempting to reduce its probability or impact. Risk acceptance does not simply ignore or remain unaware of the risks. Example: A particular project will not deliver expected results by the planned completion date. Management may decide to take this risk and continue the project. 14 Copyright 2016 ISACA. All rights reserved ID: 12355 Risk reduction Action must be taken to reduce the risk. Reducing risk to acceptable risk matching you may need to use multiple controls. Examples: Strengthening common risk management practices The introduction of a new access control system by installing new technical controls 15 Copyright 2016 ISACA. All rights reserved ID: 12355 Risk avoidance In order to avoid risks, the company will withdraw from the activities or conditions of the risk. Avoidance often has to be implemented when there is no other cost-effective response to the risks that management considers unacceptable. Example: The master data operations center is moved from a region with significant natural hazards. 16 Copyright 2016 ISACA. All rights reserved ID: 12355 Risk sharing To share the risk, you can transfer some or all of the risk effects to another organization. Examples: The organization buys fire insurance, which will pay for the replacement of structures in the event of fire. Two companies with additional skills work with each other to bid for a large project, reducing the risk that one working company would not be able to perform the contract. 17 Copyright 2016 ISACA. All rights reserved ID: 12355 Source of risk response process: ISACA, COBIT 5 for Risk, USA, 2013, 42 18 counts Copyright 2016 ISACA. All rights reserved ID: 12355 The global financial institution has decided not to take any further action on the vulnerability of the service waiver (DOS) found by the risk assessment group. The most likely reason to make this decision is that: A. the need for retaliation is too difficult to deploy. B. there are sufficient safeguards to prevent this risk from happening again. The probability of developing a C. risk is unknown. D. The cost of retaliatory measures exceeds the value of the asset and the potential loss. Discussion issue 19 Copyright 2016 ISACA. All rights reserved ID: 12355 The risk response report shall include recommendations for: A. acceptance. B. Assessment. C. Evaluation. D. quantification. Discussion issue 20 Copyright 2016 ISACA. All rights reserved ID: 12355 Task 3.2 To consult or assist risk owners in drawing up risk action plans to ensure that the plans include key elements (e.g. response, costs, target date). 21 Copyright 2016 ISACA. All rights reserved ID: 12355 How does Task 3.2 relate to each of these statements of knowledge? Task knowledge statement knowledge statement connection 9. Standards for risk identification and classification and systems Standards and systems are reproduced in the methodology for determining and classifying risks associated with that particular. 23. Risk and control ownership principles Each risk scenario should be assigned to the risk owner in order to ensure that the scenario is thoroughly examined. 29. Systems control design and implementation, including test methodologies and practices Although the control owner is responsible for the effectiveness of controls, it is essential that control measures are designed to achieve control objectives. 22 Copyright 2016 ISACA. All rights reserved ID: 12355 Selecting The choice of controls is influenced by various factors. This may be: Current risk risk Regulations Strategic plans Budget, staff and time constraints Public pressure Competitors actions Selected controls should be aligned with corporate culture, technology, budget and strategy. They should also provide accurate, timely information and be effective and measurable. 23 Copyright 2016 ISACA ISACA