

# ISACA CRISC Passleader Review & CRISC Latest Dumps Ebook



P.S. Free 2026 ISACA CRISC dumps are available on Google Drive shared by ITPassLeader: <https://drive.google.com/open?id=1usxilS9Zelg6DcOj-Zd-OwGFcscoA9qj>

It is heartening to announce that all ISACA users will be allowed to capitalize on a free ISACA CRISC exam questions demo of all three formats of ISACA CRISC practice test. It will make them scrutinize how our formats work and what we offer them, for example, the form and pattern of ISACA CRISC Exam Dumps, and their relevant and updated answers.

In order to meet the needs of all people, the experts of our company designed such a CRISC guide torrent that can help you pass your exam successfully. Having our study materials, it will be very easy for you to get the certification in a short time. If you try purchase our study materials, you will find our CRISC question torrent will be very useful for you. We are confident that you will be attracted to our CRISC guide question.

>> ISACA CRISC Passleader Review <<

## ISACA CRISC Latest Dumps Ebook & CRISC Latest Version

As we all know, the influence of CRISC exam guides even have been extended to all professions and trades in recent years. Passing the CRISC exam is not only for obtaining a paper certification, but also for a proof of your ability. Most people regard ISACA certification as a threshold in this industry, therefore, for your convenience, we are fully equipped with a professional team with specialized experts to study and design the most applicable CRISC exam prepare. We have organized a team to research and study question patterns pointing towards various learners. Our company keeps pace with contemporary talent development and makes every learners fit in the needs of the society. Based on advanced technological capabilities, our CRISC Study Materials are beneficial for the masses of customers. Our experts have plenty of experience in meeting the requirement of our customers and try to deliver satisfied CRISC exam guides to them. Our CRISC exam prepare is definitely better choice to help you go through the test.

The CRISC certification covers four key domains: IT risk identification, IT risk assessment, risk response and mitigation, and risk and control monitoring and reporting. CRISC exam tests candidates' knowledge of these domains and their ability to apply this knowledge to real-world situations. The CRISC certification is highly regarded by employers and demonstrates that an individual has the knowledge and skills required to manage risks associated with information systems. In addition to enhancing career prospects, the CRISC Certification provides individuals with the confidence and expertise required to effectively manage information systems risk within their organizations.

## ISACA Certified in Risk and Information Systems Control Sample Questions (Q701-Q706):

### NEW QUESTION # 701

The PRIMARY objective of a risk identification process is to:

- A. estimate anticipated financial impact of risk conditions.
- B. evaluate how risk conditions are managed.
- C. establish risk response options.
- D. determine threats and vulnerabilities.

**Answer: D**

Explanation:

The primary objective of a risk identification process is to determine threats and vulnerabilities, which are the sources and causes of the risks that may affect the organization's objectives. Threats are any events or circumstances that have the potential to harm or exploit the organization's assets, such as people, information, systems, processes, or infrastructure<sup>1</sup>. Vulnerabilities are any weaknesses or gaps in the organization's capabilities, controls, or defenses that may increase the likelihood or impact of the threats<sup>2</sup>. By determining threats and vulnerabilities, the organization can:

Identify and document all possible risks, regardless of whether they are internal or external, current or emerging, or positive or negative<sup>3</sup>.

Understand the nature and characteristics of the risks, such as their sources, causes, consequences, and interrelationships<sup>4</sup>.

Provide the basis for further risk analysis and evaluation, such as assessing the probability and severity of the risks, and prioritizing the risks according to their significance and urgency<sup>5</sup>.

References =

Threat - CIO Wiki

Vulnerability - CIO Wiki

Risk Identification - CIO Wiki

Risk Identification and Analysis - The National Academies Press

Risk Analysis - CIO Wiki

## NEW QUESTION # 702

Which of the following methods is an example of risk mitigation?

- A. Not providing capability for employees to work remotely
- **B. Enforcing change and configuration management processes**
- C. Taking out insurance coverage for IT-related incidents
- D. Outsourcing the IT activities and infrastructure

**Answer: B**

Explanation:

Risk mitigation is a proactive business strategy to identify, assess, and mitigate potential threats or uncertainties that could harm an organization's objectives, assets, or operations<sup>1</sup>. It entails specific action plans to reduce the likelihood or impact of these identified risks<sup>2</sup>.

There are several recognized ways to mitigate risk, such as accepting, avoiding, hedging, transferring, or reducing the risk<sup>3</sup>. Among the options given, only C is an example of risk reduction, which involves implementing controls or safeguards to minimize the negative effects of the risk<sup>3</sup>. Change and configuration management processes are methods to ensure that changes to the IT systems or infrastructure are properly authorized, documented, tested, and implemented, and that the configuration of the IT assets is consistent and accurate. These processes can help prevent or detect errors, defects, or vulnerabilities that could compromise the IT performance, security, or availability.

The other options are not examples of risk mitigation, but rather risk avoidance (A), risk transfer (B), or risk acceptance (D). Risk avoidance means eliminating the risk entirely by not engaging in the activity that causes the risk<sup>3</sup>. Not providing capability for employees to work remotely could avoid the risk of data breaches or network issues, but it could also limit the productivity and flexibility of the workforce. Risk transfer means shifting the responsibility or burden of the risk to another party, such as a vendor or an insurer<sup>3</sup>. Outsourcing the IT activities and infrastructure could transfer the risk of IT failures or incidents to the service provider, but it could also introduce new risks such as vendor dependency or loss of control. Risk acceptance means acknowledging the risk and its consequences without taking any action to address it<sup>3</sup>. Taking out insurance coverage for IT-related incidents could provide some financial compensation in case of a loss, but it does not reduce the likelihood or impact of the risk itself. References =

5 Key Risk Mitigation Strategies (With Examples) | Indeed.com

10 Risk Mitigation techniques you need to know - Stakeholdermap.com

Risk Mitigation Strategies: Types & Examples (+ Free Template)

[Change and Configuration Management - ISACA]

### NEW QUESTION # 703

Which of the following should be the PRIMARY basis for deciding whether to disclose information related to risk events that impact external stakeholders?

- A. Stakeholder preferences
- B. Contractual requirements
- C. Management assertions
- **D. Regulatory requirements**

**Answer: D**

Explanation:

Regulatory requirements should be the primary basis for deciding whether to disclose information related to risk events that impact external stakeholders, because they define the rules or standards that the organization must comply with to meet the expectations of the regulators, such as government agencies or industry bodies, and to avoid legal or reputational consequences. A risk event is an occurrence or incident that may cause harm or damage to the organization or its objectives, such as a natural disaster, a cyberattack, or a human error. An external stakeholder is a person or group that has an interest or influence in the organization or its activities, but is not part of the organization, such as customers, suppliers, partners, investors, or regulators. Disclosing information related to risk events that impact external stakeholders is a process of communicating or reporting the relevant facts or details of the risk events to the affected or interested parties. Disclosing information related to risk events may have benefits, such as maintaining trust, transparency, and accountability, but it may also have drawbacks, such as exposing vulnerabilities, losing competitive advantage, or inviting litigation.

Therefore, regulatory requirements should be the primary basis for deciding whether to disclose information, as they provide the legal and ethical obligations and boundaries for the disclosure process. Stakeholder preferences, contractual requirements, and management assertions are all possible factors for deciding whether to disclose information related to risk events, but they are not the primary basis, as they may vary or conflict depending on the situation or context, and may not override the regulatory requirements.

References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

### NEW QUESTION # 704

An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

- **A. Organizational policy**
- B. Employee code of conduct
- C. Industry best practices
- D. Organizational strategy

**Answer: A**

Explanation:

The best answer is D. Organizational policy. An organizational policy is a set of rules and guidelines that defines how the organization operates and conducts its activities. An organizational policy should direct how the employee monitoring system is used, because it can specify the purpose, scope, methods, and limitations of the monitoring, as well as the roles and responsibilities of the parties involved, the data protection and privacy measures, and the consequences of non-compliance. An organizational policy can also help to ensure that the employee monitoring system is aligned with the organization's objectives, values, and culture, and that it complies with the relevant laws and regulations. The other options are not the best answer, although they may be related or influential to the organizational policy. Organizational strategy is a plan of action that outlines the organization's vision, mission, goals, and initiatives, but it does not provide the details or the rules of how the employee monitoring system is used. Employee code of conduct is a document that describes the expected behavior and ethics of the employees, but it does not address the specific aspects or the procedures of the employee monitoring system. Industry best practices are the proven methods and standards that are adopted by the leading organizations in a specific field or sector, but they may not be applicable or suitable for every organization or situation.

References = Workplace Monitoring Policy Template - CurrentWare, The All-In-One Guide to Employee Monitoring - G2

### NEW QUESTION # 705

A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

- A. invoke the established incident response plan.
- B. Inform internal audit.

- Answer: D**

• • • • •

**CRISC Latest Dumps Ebook:** <https://www.itpassleader.com/ISACA/CRISC-dumps-pass-exam.html>

- BTW, DOWNLOAD part of ITPassLeader CRISC dumps from Cloud Storage: <https://drive.google.com/open?id=1usxliS9Zelg6DcOj-Zd-OwGFcscoA9qj>