



# CRISC<sup>Q&As</sup>

Certified in Risk and Information Systems Control

## Pass Isaca CRISC Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/crisc.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

Which of the following is the MOST relevant input to an organization's risk profile?

- A. External audit's risk assessment
- B. Management's risk self-assessment
- C. Internal audit's risk assessment
- D. Information security's vulnerability assessment

Correct Answer: A

---

### QUESTION 2

In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

- A. two-factor authentication.
- B. continuous data backup controls.
- C. encryption for data at rest.
- D. encryption for data in motion.

Correct Answer: B

---

### QUESTION 3

The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.



Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise.	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile devices
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
		A disgruntled								
Significant					0.10	Low Likelihood				0.30
Serious					0.20	Likely				0.50
Very Serious					0.40	Highly Likely				0.70
Catastrophic					0.80	Near Certainty				0.90

After implementing countermeasures listed in 'Risk Response Descriptions' for each of the Risk IDs, which of the following component of the register MUST change?

- A. Risk Impact Rating
- B. Risk Owner
- C. Risk Likelihood Rating
- D. Risk Exposure

Correct Answer: B

#### QUESTION 4

You and your project team have identified a few risk events in the project and recorded the events in the risk register. Part of the recording of the events includes the identification of a risk owner. Who is a risk owner?

- A. A risk owner is the party that will monitor the risk events.
- B. A risk owner is the party that will pay for the cost of the risk event if it becomes an issue.
- C. A risk owner is the party that has caused the risk event.
- D. A risk owner is the party authorized to respond to the risk event.



Correct Answer: D

---

#### QUESTION 5

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.
- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

Correct Answer: A

[Latest CRISC Dumps](#)

[CRISC PDF Dumps](#)

[CRISC Braindumps](#)