

CISA^{Q&As}

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

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

<https://www.leads4pass.com/cisa.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

During a review of the IT strategic plan, an IS auditor finds several IT initiatives focused on delivering new systems and technology are not aligned with the organization's strategy. Which of the following would be the IS auditor's BEST recommendation?

- A. Reassess the return on investment for the IT initiatives
- B. Modify IT initiatives that do not map to business strategies
- C. Utilize a balanced scorecard to align IT initiatives to business strategies
- D. Reassess IT initiatives that do not map business strategies

Correct Answer: D

QUESTION 2

What would be an IS auditor's BEST course of action when an auditee is unable to close all audit recommendations by the time of the follow-up audit?

- A. Ensure the open issues are retained in the audit results.
- B. Terminate the follow-up because open issues are not resolved
- C. Recommend compensating controls for open issues.
- D. Evaluate the residual risk due to open issues.

Correct Answer: D

QUESTION 3

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

- A. manual processing capabilities and the test location.
- B. the importance of the function to be tested and the cost of testing.
- C. the experience level of personnel and the function location.
- D. prior testing results and the degree of detail of the business continuity plan.

Correct Answer: B

QUESTION 4

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- A. Loss of application support
- B. Lack of system integrity
- C. Outdated system documentation
- D. Developer access to production

Correct Answer: B

QUESTION 5

Which of the following audit risk is related to material errors or misstatements that have occurred that will not be detected by an IS auditor?

- A. Inherent Risk
- B. Control Risk
- C. Detection Risk
- D. Overall Audit Risk

Correct Answer: C

The risk that material errors or misstatements that have occurred will not be detected by an IS auditor. Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements. An auditor must apply audit

procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some

detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions. Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed

testing.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control

risk (CR) and detection risk (DR), and can be calculated thus:

$$AR = IR \times CR \times DR$$

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial

statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement

assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

Rapid change: A business whose inventory becomes obsolete quickly experiences high inherent risk.

Expiring patents: Any business in the pharmaceutical industry also has inherently risky environment and external factors. Drug patents eventually expire, which means the company faces competition from other manufacturers marketing the

same drug under a generic label.

State of the economy: The general level of economic growth is another external factor affecting all businesses.

Availability of financing: Another external factor is interest rates and the associated availability of financing. If your client is having problems meeting its short-term cash payments, available loans with low interest rates may mean the difference

between your client staying in business or having to close its doors.

Prior-period misstatements: If a company has made mistakes in prior years that weren't material (meaning they weren't significant enough to have to change), those errors still exist in the financial statements. You have to aggregate prior-

period misstatements with current year misstatements to see if you need to ask the client to adjust the account for the total misstatement.

You may think an understatement in one year compensates for an overstatement in another year. In auditing, this assumption isn't true. Say you work a cash register and one night the register comes up \$20 short. The next week, you

somehow came up \$20 over my draw count. The \$20 differences are added together to represent the total amount of your mistakes which is \$40 and not zero. Zero would indicate no mistakes at all had occurred.

Susceptibility to theft or fraud: If a certain asset is susceptible to theft or fraud, the account or balance level may be considered inherently risky. For example, if a client has a lot of customers who pay in cash, the balance sheet cash account is

going to have risk associated with theft or fraud because of the fact that cash is more easily diverted than customer checks or credit card payments.

Looking at industry statistics relating to inventory theft, you may also decide to consider the inventory account as inherently risky. Small inventory items can further increase the risk of this account valuation being incorrect because those items

are easier to conceal (and therefore easier to steal).

Control Risk

Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or

detected and corrected, on a timely basis by the entity's internal control.

In simple words control risk is the probability that a material misstatement exists in an assertion because that misstatement was not either prevented from entering entity's financial information or it was not detected and corrected by the

internal control system of the entity.

It is the responsibility of the management and those charged with governance to implement internal control system and maintain it appropriately which includes managing control risk.

There can be many reasons for control risk to arise and why it cannot be eliminated absolutely. But some of them are as follows:

Cost-benefit constraints

Circumvention of controls

Inappropriate design of controls

Inappropriate application of controls

Lack of control environment and accountability

Novel situations

Outdated controls

Inappropriate segregation of duties

Detection Risk

Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements.

An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining

undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.

Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

The following answers are incorrect:

Inherent Risk - It is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented.

Control Risk - The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls.

Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area

under security so the overall audit risk is at sufficiently low level at the completion of the examination.

Reference:

CISA review manual 2014 page number 50

http://en.wikipedia.org/wiki/Audit_risk

<http://www.dummies.com/how-to/content/how-to-assess-inherent-risk-in-an-audit.html>

<http://pakaccountants.com/what-is-control-risk/>

<http://accounting-simplified.com/audit/risk-assessment/audit-risk.html>

[CISA VCE Dumps](#)

[CISA Practice Test](#)

[CISA Exam Questions](#)