

Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. ALE calculations are only valid if assets have first been identified and appropriately valued. Motives, means and opportunities should already be factored in as a part of a risk assessment.

QUESTION 234

The criticality and sensitivity of information assets is determined on the basis of:

- A. threat assessment.
- B. vulnerability assessment.
- C. resource dependency assessment.
- D. impact assessment.

Correct Answer: D

Explanation:

The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

QUESTION 235

To determine the selection of controls required to meet business objectives, an information security manager should:

- A. prioritize the use of role-based access controls.
- B. focus on key controls.
- C. restrict controls to only critical applications.
- D. focus on automated controls.

Correct Answer: B

Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

QUESTION 236

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- A. Risk analysis process
- B. Business impact analysis (BIA)
- C. Risk management balanced scorecard
- D. Risk-based audit program

Correct Answer: B

Explanation:

[CISM Exam Dumps](#) **[CISM PDF Dumps](#) **[CISM VCE Dumps](#) **[CISM Q&As](#)******

<https://www.ensurepass.com/CISM.html>

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

QUESTION 237

When a significant security breach occurs, what should be reported FIRST to senior management?

- A. A summary of the security logs that illustrates the sequence of events
- B. An explanation of the incident and corrective action taken
- C. An analysis of the impact of similar attacks at other organizations
- D. A business case for implementing stronger logical access controls

Correct Answer: B

Explanation:

When reporting an incident to senior management, the initial information to be communicated should include an explanation of what happened and how the breach was resolved. A summary of security logs would be too technical to report to senior management. An analysis of the impact of similar attacks and a business case for improving controls would be desirable; however, these would be communicated later in the process.

QUESTION 238

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

- A. Justification of the security budget must be continually made.
- B. New vulnerabilities are discovered every day.
- C. The risk environment is constantly changing.
- D. Management needs to be continually informed about emerging risks.

Correct Answer: C

Explanation:

The risk environment is impacted by factors such as changes in technology, and business strategy. These changes introduce new threats and vulnerabilities to the organization. As a result, risk assessment should be performed continuously. Justification of a budget should never be the main reason for performing a risk assessment. New vulnerabilities should be managed through a patch management process. Informing management about emerging risks is important, but is not the main driver for determining when a risk assessment should be performed.

QUESTION 239

Which two components PRIMARILY must be assessed in an effective risk analysis?

- A. Visibility and duration
- B. Likelihood and impact
- C. Probability and frequency
- D. Financial impact and duration

Correct Answer: B

Explanation:

The probability or likelihood of the event and the financial impact or magnitude of the event must be assessed first. Duration refers to the length of the event; it is important in order to assess impact but is secondary. Once the likelihood is determined, the frequency is also important to determine overall impact.

QUESTION 240

Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

- A. Tree diagrams
- B. Venn diagrams
- C. Heat charts
- D. Bar charts

Correct Answer: C

Explanation:

Heat charts, sometimes referred to as stoplight charts, quickly and clearly show the current status of remediation efforts. Venn diagrams show the connection between sets; tree diagrams are useful for decision analysis; and bar charts show relative size.

QUESTION 241

Which of the following steps in conducting a risk assessment should be performed FIRST?

- A. Identify business assets
- B. Identify business risks
- C. Assess vulnerabilities
- D. Evaluate key controls

Correct Answer: A

Explanation:

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

QUESTION 242

Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

- A. conduct a risk assessment and allow or disallow based on the outcome.
- B. recommend a risk assessment and implementation only if the residual risks are accepted.
- C. recommend against implementation because it violates the company's policies.
- D. recommend revision of current policy.

Correct Answer: B

Explanation:

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

QUESTION 243

Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

- A. Strategic business plan
- B. Upcoming financial results
- C. Customer personal information
- D. Previous financial results

Correct Answer: D

Explanation:

Previous financial results are public; all of the other choices are private information and should only be accessed by authorized entities.

QUESTION 244

The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

- A. determining the scope for inclusion in an information security program.
- B. defining the level of access controls.
- C. justifying costs for information resources.
- D. determining the overall budget of an information security program.

Correct Answer: B

Explanation:

The assigned class of sensitivity and criticality of the information resource determines the level of access controls to be put in place. The assignment of sensitivity and criticality takes place with the information assets that have already been included in the information security program and has only an indirect bearing on the costs to be incurred. The assignment of sensitivity and criticality contributes to, but does not decide, the overall budget of the information security program.

QUESTION 245

Acceptable risk is achieved when:

- A. residual risk is minimized.
- B. transferred risk is minimized.
- C. control risk is minimized.
- D. inherent risk is minimized.

Correct Answer: A

Explanation:

Residual risk is the risk that remains after putting into place an effective risk management program; therefore, acceptable risk is achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party and may not necessarily be equal to the minimal form of residual risk. Control risk is the risk that controls may not prevent/detect an incident with a measure of control effectiveness. Inherent risk cannot be minimized.

QUESTION 246

Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

[CISM Exam Dumps](#) [CISM PDF Dumps](#) [CISM VCE Dumps](#) [CISM Q&As](#)

<https://www.ensurepass.com/CISM.html>

- A. Performing a business impact analysis (BIA)
- B. Considering personal information devices as part of the security policy
- C. Initiating IT security training and familiarization
- D. Basing the information security infrastructure on risk assessment

Correct Answer: D

Explanation:

The information security infrastructure should be based on risk. While considering personal information devices as part of the security policy may be a consideration, it is not the most important requirement. A BIA is typically carried out to prioritize business processes as part of a business continuity plan. Initiating IT security training may not be important for the purpose of the information security infrastructure.

QUESTION 247

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

- A. Countermeasure cost-benefit analysis
- B. Penetration testing
- C. Frequent risk assessment programs
- D. Annual loss expectancy (ALE) calculation

Correct Answer: A

Explanation:

In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control. Frequent risk assessment programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will contribute to the value of the risk but, alone, will not justify a control.

QUESTION 248

The MOST effective way to incorporate risk management practices into existing production systems is through:

- A. policy development.
- B. change management.
- C. awareness training.
- D. regular monitoring.

Correct Answer: B

Explanation:

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

QUESTION 249

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should: