

QUESTIONS & ANSWERS

Kill your exam at first Attempt

CRISC Dumps
CRISC Braindumps
CRISC Real Questions
CRISC Practice Test
CRISC dumps free



ISACA

CRISC

Certified in Risk and Information Systems Control



<https://killexams.com/pass4sure/exam-detail/CRISC>

Question #910

Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

- A. Use of industry risk data sources
- B. Sensitivity to changes in risk levels
- C. Low cost of development and maintenance
- D. Approval by senior management

Answer: A

Question #911

Which of the following is the BEST indication of a mature organizational risk culture?

- A. Corporate risk appetite is communicated to staff members.
- B. Risk policy has been published and acknowledged by employees.
- C. Management encourages the reporting of policy breaches.
- D. Risk owners understand and accept accountability for risk.

Answer: D

Question #912

The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

- A. active accounts belonging to former personnel.
- B. accounts with dormant activity.
- C. accounts without documented approval.
- D. user accounts with default passwords.

Answer: A

Question #913

Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

- A. Segregation of duties
- B. Compliance review
- C. Three lines of defense
- D. Quality assurance review

Answer: C

Question #914

Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

- A. Third-party AI solutions increase regulatory obligations.
- B. AI requires entirely new risk management processes.
- C. AI will result in changes to business processes.
- D. AI potentially introduces new types of risk.

Answer: D

Question #915

An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

- A. Mitigation
- B. Acceptance
- C. Avoidance
- D. Transfer

Answer: B

Question #916

To communicate the risk associated with IT in business terms, which of the following **MUST** be defined?

- A. Risk appetite of the organization
- B. Compliance objectives
- C. Organizational objectives
- D. Inherent and residual risk

Answer: C

Question #917

An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done **FIRST** to reduce the likelihood of infection from the attack?

- A. Verify the data backup process and confirm which backups are the most recent ones available.
- B. Identify systems that are vulnerable to being exploited by the attack.
- C. Confirm with the antivirus solution vendor whether the next update will detect the attack.
- D. Obtain approval for funding to purchase a cyber insurance plan.

Answer: B

Question #918

Which of the following is **MOST** important to the successful development of IT risk scenarios?

- A. Control effectiveness assessment
- B. Threat and vulnerability analysis
- C. Internal and external audit reports
- D. Cost-benefit analysis

Answer: D

Question #919

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially. Which of the following would be the **BEST** approach for the risk practitioner to take?

- A. Temporarily suspend emergency changes.
- B. Continue monitoring change management metrics.
- C. Conduct a root cause analysis.
- D. Document the control deficiency in the risk register.

Answer: C

Question #920

Which of the following **MUST** be updated to maintain an IT risk register?

- A. Risk appetite
- B. Risk tolerance
- C. Expected frequency and potential impact
- D. Enterprise-wide IT risk assessment

Answer: C

Question #921

Which of the following is the **BEST** method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

- A. Vulnerability scanning
- B. Penetration testing
- C. Systems log correlation analysis
- D. Monitoring of intrusion detection system (IDS) alerts

Answer: B

Question #922

Which of the following is the **MOST** effective control to ensure user access is maintained on a least-privilege basis?

- A. Change log review
- B. User recertification
- C. Access log monitoring
- D. User authorization

Answer: D

Question #923

Which of the following is **MOST** important when considering risk in an enterprise risk management (ERM) process?

- A. Risk identified by industry benchmarking is included.
- B. Financial risk is given a higher priority.
- C. Risk with strategic impact is included.
- D. Security strategy is given a higher priority.

Answer: C

Question #924

Which of the following is **MOST** important when developing risk scenarios?

- A. Conducting vulnerability assessments
- B. Reviewing business impact analysis (BIA)
- C. Collaborating with IT audit
- D. Obtaining input from key stakeholders

Answer: B

Question #925

Which of the following **BEST** protects an organization against breaches when using a software as a service (SaaS)

application?

- A. Security information and event management (SIEM) solutions
- B. Control self-assessment (CSA)
- C. Data privacy impact assessment (DPIA)
- D. Data loss prevention (DLP) tools

Answer: D

Question #926

Which of the following is the GREATEST risk associated with the misclassification of data?

- A. Data disruption
- B. Inadequate resource allocation
- C. Unauthorized access
- D. Inadequate retention schedules

Answer: C

Question #927

Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

- A. Disabling social media access from the organization's technology
- B. Validating employee social media accounts and passwords
- C. Implementing training and awareness programs
- D. Monitoring Internet usage on employee workstations

Answer: C

Question #928

Which of the following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

- A. Perform a risk assessment.
- B. Prioritize impact to the business units.
- C. Perform a gap analysis.
- D. Review the risk tolerance and appetite.

Answer: C

Question #929

The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

- A. benchmarking criteria.
- B. stakeholder risk tolerance.
- C. the control environment.
- D. suppliers used by the organization.

Answer: A

Question #930

A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

- A. Require the software vendor to remediate the vulnerabilities.
- B. Approve exception to allow the software to continue operating.
- C. Monitor the databases for abnormal activity.
- D. Accept the risk and let the vendor run the software as is.

Answer: A

Question #931

Which of the following represents a vulnerability?

- A. An employee recently fired for insubordination
- B. An identity thief seeking to acquire personal financial data from an organization
- C. Media recognition of an organization's market leadership in its industry
- D. A standard procedure for applying software patches two weeks after release

Answer: D

Question #932

An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

- A. Potential increase in regulatory scrutiny
- B. Potential theft of personal information
- C. Potential legal risk
- D. Potential system downtime

Answer: B

Question #933

Which of the following is the PRIMARY role of a data custodian in the risk management process?

- A. Ensuring data is protected according to the classification
- B. Being accountable for control design
- C. Reporting and escalating data breaches to senior management
- D. Performing periodic data reviews according to policy

Answer: A

For More exams visit <https://killexams.com/vendors-exam-list>



Kill your exam at First Attempt....Guaranteed!