VCEplus
VCE To PDF - Free Practice Exam

712-50

Passing Score: 800
Time Limit: 0 min

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

https://vceplus.com/

VCEplus
VCE To PDF - Free Practice Exam

Exam A

QUESTION 1
Credit card information, medical data, and government records are all examples of:

https://vceplus.com/

A. Confidential/Protected Information
B. Bodily Information
C. Territorial Information
D. Communications Information

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 2
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope
B. Getting authority to operate the system from executive management
C. Changing the default passwords
D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 3
The single most important consideration to make when developing your security program, policies, and processes is:
A. Budgeting for unforeseen data compromises
B. Streamlining for efficiency
C. Alignment with the business
D. Establishing your authority as the Security Executive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
An organization's Information Security Policy is of MOST importance because

A. it communicates management's commitment to protecting information resources
B. it is formally acknowledged by all employees and vendors
C. it defines a process to meet compliance requirements
D. it establishes a framework to protect confidential information

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Developing effective security controls is a balance between:

A. Risk Management and Operations
B. Corporate Culture and Job Expectations
C. Operations and Regulations
D. Technology and Vendor Management

Correct Answer: A

www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation
Explanation/Reference:

QUESTION 6
The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.
B. Establishing strategic alignment with bunsiness continuity requirements
C. Establishing incident response programs.
D. Identifying and implementing the best security solutions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 7
Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance
B. Risk assessment criteria
C. IT architecture complexity
D. Enterprise disaster recovery plans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Who in the organization determines access to information?

VCEplus
VCE To PDF - Free Practice Exam

A. Legal department
B. Compliance officer
C. Data Owner
D. Information security officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is a benefit of information security governance?

A. Questioning the trust in vendor relationships.
B. Increasing the risk of decisions based on incomplete management information.
C. Direct involvement of senior management in developing control processes
D. Reduction of the potential for civil and legal liability

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following is the MOST important benefit of an effective security governance process?

VCEplus
VCE To PDF - Free Practice Exam

A. Reduction of liability and overall risk to the organization
B. Better vendor management
C. Reduction of security breaches
D. Senior management participation in the incident response process

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.
B. Obtain senior level sponsorship.
C. Conduct a workshop for all end users.
D. Prepare a security budget.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following has the GREATEST impact on the implementation of an information security governance model?

A. Organizational budget
B. Distance between physical locations
C. Number of employees
D. Complexity of organizational structure

Correct Answer: D

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. assessed by a business impact analysis.

B. protected under the information classification policy.
C. analyzed under the data ownership policy.
D. analyzed under the retention policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 14
When briefing senior management on the creation of a governance process, the MOST important aspect should be:

A. information security metrics.
B. knowledge required to analyze each issue.
C. baseline against which metrics are evaluated.
D. linkage to business area objectives.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

VCEplus
VCE To PDF - Free Practice Exam

Which of the following most commonly falls within the scope of an information security governance steering committee?

A. Approving access to critical financial systems
B. Developing content for security awareness programs
C. Interviewing candidates for information security specialist positions
D. Vetting information security policies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 16
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

A. Lack of a formal security awareness program
B. Lack of a formal security policy governance process
C. Lack of formal definition of roles and responsibilities
D. Lack of a formal risk management policy

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

A. Need to comply with breach disclosure laws
B. Need to transfer the risk associated with hosting PII data
C. Need to better understand the risk associated with using PII data
D. Fiduciary responsibility to safeguard credit card information

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The alerting, monitoring and life-cycle management of security related events is typically handled by the

A. security threat and vulnerability management process
B. risk assessment process
C. risk management process
D. governance, risk, and compliance tools

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 19
One of the MAIN goals of a Business Continuity Plan is to

A. Ensure all infrastructure and applications are available in the event of a disaster
B. Allow all technical first-responders to understand their roles in the event of a disasterC. Provide step by step plans to recover business processes in the event of a disaster
D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

VCEplus
VCE To PDF - Free Practice Exam

When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

https://vceplus.com/

A. An independent Governance, Risk and Compliance organization
B. Alignment of security goals with business goals
C. Compliance with local privacy regulations
D. Support from Legal and HR teams

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 21
Which of the following is considered the MOST effective tool against social engineering?

A. Anti-phishing tools
B. Anti-malware tools
C. Effective Security Vulnerability Management Program
D. Effective Security awareness program

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

VCEplus
VCE To PDF - Free Practice Exam

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

A. Escalation
B. Recovery
C. Eradication
D. Containment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

A. Poses a strong technical background
B. Understand all regulations affecting the organization
C. Understand the business goals of the organization
D. Poses a strong auditing background

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

A. High risk environments 6 months, low risk environments 12 months
B. Every 12 months
C. Every 18 months
D. Every six months

Correct Answer: B

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

A. Strong authentication technologies
B. Financial reporting regulations
C. Credit card compliance and regulations
D. Local privacy laws

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 26
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

VCEplus
VCE To PDF - Free Practice Exam

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Risk that remains after risk mitigation is known as

A. Persistent risk
B. Residual risk
C. Accepted risk
D. Non-tolerated risk

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

A. Risk Tolerance
B. Qualitative risk analysis
C. Risk Appetite
D. Quantitative risk analysis

Correct Answer: D
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 30
When dealing with a risk management process, asset classification is important because it will impact the overall:

VCEplus
Free Practice Exam - IT Certifications

https://vceplus.com/

A. Threat identification
B. Risk monitoring
C. Risk treatment
D. Risk tolerance

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following intellectual Property components is focused on maintaining brand recognition?

A. Trademark
B. Patent
C. Research Logs
D. Copyright

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 32
The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

A. Due Protection
B. Due Care
C. Due Compromise
D. Due process

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

VCEplus
VCE To PDF - Free Practice Exam

A. How many credit card records are stored?
B. How many servers do you have?
C. What is the scope of the certification?
D. What is the value of the assets at risk?

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What is a difference from the list below between quantitative and qualitative Risk Assessment?

A. Quantitative risk assessments result in an exact number (in monetary terms)

VCEplus
VCE To PDF - Free Practice Exam

B. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
C. Qualitative risk assessments map to business objectives
D. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What is the definition of Risk in Information Security?

A. Risk = Probability x Impact
B. Risk = Threat x Probability
C. Risk = Financial Impact x Probability
D. Risk = Impact x Threat

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 36
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

A. They are objective and can express risk / cost in real numbers
B. They are subjective and can be completed more quickly
C. They are objective and express risk / cost in approximates
D. They are subjective and can express risk /cost in real numbers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 37
Which of the following is MOST important when dealing with an Information Security Steering committee:

A. Include a mix of members from different departments and staff levels.
B. Ensure that security policies and procedures have been vetted and approved.
C. Review all past audit and compliance reports.
D. Be briefed about new trends and products at each meeting by a vendor.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

VCEplus
VCE To PDF - Free Practice Exam

A. Enforce the existing security standards and do not allow the deployment of the new technology.
B. Amend the standard to permit the deployment.
C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
The PRIMARY objective of security awareness is to:

A. Ensure that security policies are read.
B. Encourage security-conscious employee behavior.
C. Meet legal and regulatory requirements.

VCEplus
VCE To PDF - Free Practice Exam

D. Put employees on notice in case follow-up action for noncompliance is necessary

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is MOST likely to be discretionary?

https://vceplus.com/

VCEplus
VCE To PDF - Free Practice Exam

A. Policies
B. Procedures
C. Guidelines
D. Standards

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Why is it vitally important that senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.

VCEplus
VCE To PDF - Free Practice Exam

D. So that they can be held legally accountable.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

A. When there is a need to develop a more unified incident response capability.
B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
C. When there is a variety of technologies deployed in the infrastructure.
D. When it results in an overall lower cost of operating the security program.

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 43
What is the relationship between information protection and regulatory compliance?

A. That all information in an organization must be protected equally.

B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protectedbased on business need.
D. There is no relationship between the two.

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 44
Regulatory requirements typically force organizations to implement

A. Mandatory controls
B. Discretionary controls
C. Optional controls
D. Financial controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
When managing the security architecture for your company you must consider:

VCEplus
VCE To PDF - Free Practice Exam

A. Security and IT Staff size
B. Company Values
C. Budget
D. All of the above

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 46
If your organization operates under a model of "assumption of breach", you should:

A. Protect all information resource assets equally
B. Establish active firewall monitoring protocols
C. Purchase insurance for your compliance liabilityD. Focus your security efforts on high value assets

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A method to transfer risk is to:

A. Implement redundancy
B. move operations to another region
C. purchase breach insurance
D. Alignment with business operations

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 48
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

A. Controlled mitigation effort
B. Risk impact comparison
C. Relative likelihood of event
D. Comparative threat analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

VCEplus
VCE To PDF - Free Practice Exam

Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

A. Risk management
B. Security management
C. Mitigation management
D. Compliance management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A security manager regualrly checks work areas after buisness hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

VCEplus
VCE To PDF - Free Practice Exam

https://vceplus.com/

A. Audit validation
B. Physical control testing
C. Compliance management
D. Security awareness training

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 51
A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

A. Internal audit
B. The data owner
C. All executive staff
D. Government regulators

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

VCEplus
VCE To PDF - Free Practice Exam

A. Multiple certifications, strong technical capabilities and lengthy resume
B. Industry certifications, technical knowledge and program management skills
C. College degree, audit capabilities and complex project management
D. Multiple references, strong background check and industry certifications

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

A. Data breach disclosure
B. Consumer right disclosure

www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

VCEplus
VCE To PDF - Free Practice Exam

C. Security incident disclosure
D. Special circumstance disclosure

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

A. A high threat environment
B. A low risk tolerance environment
C. I low vulnerability environment
D. A high risk tolerance environment

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

A. Determine the risk tolerance
B. Perform an asset classification
C. Create an architecture gap analysis
D. Analyze existing controls on systems
Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 56
A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

A. Providing a risk program governance structure
B. Ensuring developers include risk control comments in code
C. Creating risk assessment templates based on specific threats
D. Allowing for the acceptance of risk for regulatory compliance requirements

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

VCEplus
VCE To PDF - Free Practice Exam

A. National Institute for Standards and Technology 800-50 (NIST 800-50)
B. International Organization for Standardizations – 27005 (ISO-27005)C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27004 (ISO-27004)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?
A. International Organization for Standardizations – 27004 (ISO-27004)
B. Payment Card Industry Data Security Standards (PCI-DSS)

VCEplus
VCE To PDF - Free Practice Exam

C. Control Objectives for Information Technology (COBIT)
D. International Organization for Standardizations – 27005 (ISO-27005)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

A. Information Technology Infrastructure Library (ITIL)
B. International Organization for Standardization (ISO) standards
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. National Institute for Standards and Technology (NIST) standard

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

https://vceplus.com/

A. International Organization for Standardizations – 22301 (ISO-22301)

VCEplus
VCE To PDF - Free Practice Exam

B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations – 27005 (ISO-27005)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

A. Compliance to the Payment Card Industry (PCI) regulations.
B. Alignment with financial reporting regulations for each country where they operate.
C. Alignment with International Organization for Standardization (ISO) standards.
D. Compliance with patient data protection regulations for each country where they operate.

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

A. The organization uses exclusively a quantitative process to measure risk
B. The organization uses exclusively a qualitative process to measure risk
C. The organization's risk tolerance is high
D. The organization's risk tolerance is lo

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 63

The exposure factor of a threat to your organization is defined by?

A. Asset value times exposure factor
B. Annual rate of occurrence
C. Annual loss expectancy minus current cost of controls
D. Percentage of loss experienced due to a realized threat event

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64

Risk is defined as:

VCEplus
VCE To PDF - Free Practice Exam

A. Threat times vulnerability divided by control
B. Advisory plus capability plus vulnerability
C. Asset loss times likelihood of event
D. Quantitative plus qualitative impact

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65

What two methods are used to assess risk impact?

A. Cost and annual rate of expectance
B. Subjective and Objective
C. Qualitative and percent of loss realized
D. Quantitative and qualitative

www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

A. Identify threats, risks, impacts and vulnerabilities
B. Decide how to manage risk
C. Define the budget of the Information Security Management System
D. Define Information Security Policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 67
You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Information Security Officer
B. Chief Executive Officer
C. Chief Information Officer
D. Chief Legal Counsel

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 68
The success of the Chief Information Security Officer is MOST dependent upon:

A. favorable audit findings
B. following the recommendations of consultants and contractors
C. development of relationships with organization executives
D. raising awareness of security issues with end users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
An organization information security policy serves to

A. establish budgetary input in order to meet compliance requirements
B. establish acceptable systems and user behavior
C. define security configurations for systems
D. define relationships with external law enforcement agencies

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Information security policies should be reviewed:

VCEplus
VCE To PDF - Free Practice Exam

A. by stakeholders at least annually
B. by the CISO when new systems are brought online
C. by the Incident Response team after an audit
D. by internal audit semiannually

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Who is responsible for securing networks during a security incident?

A. Chief Information Security Officer (CISO)
B. Security Operations Center (SO
C. Disaster Recovery (DR) manager
D. Incident Response Team (IRT)

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following is a critical operational component of an Incident Response Program (IRP)?

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.
B. Annual review of program charters, policies, procedures and organizational agreements.
C. Daily monitoring of vulnerability advisories relating to your organization's deployed technologies.
D. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization

Correct Answer: C

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

Explanation/Reference:
QUESTION 73
What is the first thing that needs to be completed in order to create a security program for your organization?

A. Risk assessment
B. Security program budget
C. Business continuity plan
D. Compliance and regulatory analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 74
What is the main purpose of the Incident Response Team?

A. Ensure efficient recovery and reinstate repaired systems
B. Create effective policies detailing program activities
C. Communicate details of information security incidents
D. Provide current employee awareness programs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

A. Threat

VCEplus
VCE To PDF - Free Practice Exam

B. Vulnerability
C. Attack vector
D. Exploitation
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

A. Security officer
B. Data owner
C. Vulnerability engineer
D. System administrator

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
The Information Security Management program MUST protect:

A. all organizational assets
B. critical business processes and /or revenue streams
C. intellectual property released into the public domain
D. against distributed denial of service attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 78
What is the MAIN reason for conflicts between Information Technology and Information Security programs?
A. Technology governance defines technology policies and standards while security governance does not.
B. Security governance defines technology best practices and Information Technology governance does not.
C. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
D. The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
The Information Security Governance program MUST:

A. integrate with other organizational governance processes
B. support user choice for Bring Your Own Device (BYOD)
C. integrate with other organizational governance processes
D. show a return on investment for the organization

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

VCEplus
VCE To PDF - Free Practice Exam

VCEplus
Free Practice Exam - IT Certifications
https://vceplus.com/

A. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 81
When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

A. The asset owner
B. The asset manager
C. The data custodian
D. The project manager

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

VCEplus
VCE To PDF - Free Practice Exam

A. Audit and Legal
B. Budget and Compliance
C. Human Resources and Budget
D. Legal and Human Resources

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Risk appetite directly affects what part of a vulnerability management program?

A. Staff
B. Scope
C. Schedule
D. Scan tools

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
When choosing a risk mitigation method what is the MOST important factor?

A. Approval from the board of directors
B. Cost of the mitigation is less than the risk
C. Metrics of mitigation method success
D. Mitigation method complies with PCI regulations

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 85
Payment Card Industry (PCI) compliance requirements are based on what criteria?

A. The types of cardholder data retained
B. The duration card holder data is retained
C. The size of the organization processing credit card data
D. The number of transactions performed per year by an organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following provides an audit framework?

VCEplus
VCE To PDF - Free Practice Exam

A. Control Objectives for IT (COBIT)
B. Payment Card Industry-Data Security Standard (PCI-DSS)
C. International Organization Standard (ISO) 27002
D. National Institute of Standards and Technology (NIST) SP 800-30

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

A. Awareness

www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

VCEplus
VCE To PDF - Free Practice Exam

B. Compliance
C. Governance
D. Management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget
B. Decreased security awareness C. Improper use of information resources
D. Fines for regulatory non-compliance

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for

A. Confidentiality, Integrity and Availability
B. Assurance, Compliance and Availability
C. International Compliance
D. Integrity and Availability

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 90
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

https://vceplus.com/

A. In promiscuous mode and only detect malicious traffic.
B. In-line and turn on blocking mode to stop malicious traffic.
C. In promiscuous mode and block malicious traffic.
D. In-line and turn on alert mode to stop malicious traffic.
Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 91
What is the BEST way to achieve on-going compliance monitoring in an organization?

A. Only check compliance right before the auditors are scheduled to arrive onsite.
B. Outsource compliance to a 3rd party vendor and let them manage the program.
C. Have Compliance and Information Security partner to correct issues as they arise.
D. Have Compliance direct Information Security to fix issues after the auditors report.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 92
Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How vulnerabilities can potentially be exploited in systems that impact the organization
B. How the security operations team will behave to reported incidents
C. How the firewall and other security devices are configured to prevent attacks
D. How the incident management team prepares to handle an attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following are the MOST important factors for proactively determining system vulnerabilities?
A. Subscribe to vendor mailing list to get notification of system vulnerabilities
B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
D. Conduct security testing, vulnerability scanning, and penetration testing

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
What role should the CISO play in properly scoping a PCI environment?

A. Validate the business units' suggestions as to what should be included in the scoping process
B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
C. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data
D. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

A. Test every three years to ensure that things work as planned
B. Conduct periodic tabletop exercises to refine the BC plan
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 96
What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

A. Determine appetite
B. Evaluate risk avoidance criteria
C. Perform a risk assessment
D. Mitigate risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

VCEplus
VCE To PDF - Free Practice Exam

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

A. Susceptibility to attack, mitigation response time, and cost
B. Attack vectors, controls cost, and investigation staffing needs
C. Vulnerability exploitation, attack recovery, and mean time to repair
D. Susceptibility to attack, expected duration of attack, and mitigation availability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

VCEplus
VCE To PDF - Free Practice Exam

A. Single loss expectancy multiplied by the annual rate of occurrence
B. Total loss expectancy multiplied by the total loss frequency
C. Value of the asset multiplied by the loss expectancy
D. Replacement cost multiplied by the single loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

A. ISO 27001
B. PRINCE2
C. ISO 27004

VCEplus
VCE To PDF - Free Practice Exam

D. ITILv3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
The regular review of a firewall ruleset is considered a

VCEplus
Free Practice Exam - IT Certifications
https://vceplus.com/

VCEplus
VCE To PDF - Free Practice Exam

A. Procedural control
B. Organization control
C. Technical control
D. Management control
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

A. Organization control
B. Procedural control
C. Management control
D. Technical control

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

A. Procedural control
B. Management control
C. Technical control
D. Administrative control

Correct Answer: B
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 103
The amount of risk an organization is willing to accept in pursuit of its mission is known as

A. Risk mitigation
B. Risk transfer
C. Risk tolerance
D. Risk acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 104
Which of the following is a fundamental component of an audit record?

A. Date and time of the event
B. Failure of the event
C. Originating IP-Address
D. Authentication type

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

VCEplus
VCE To PDF - Free Practice Exam

A. Lack of notification to the public of disclosure of confidential information.
B. Lack of periodic examination of access rights
C. Failure to notify police of an attempted intrusion
D. Lack of reporting of a successful denial of service attack on the network.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

VCEplus
Free Practice Exam - IT Certifications
https://vceplus.com/