

## SelfTestEngine.CISSP-ISSMP\_218.Q&A

Number: CISSP-ISSMP

Passing Score: 800

Time Limit: 120 min

File Version: 9.02








<http://www.gratisexam.com/>



ISSMP

**ISSMP®: Information Systems Security  
Management Professional**

-  I took the exam today. All questions and sims were different.
-  This is a guaranteed pass. tried and tested
-  95% Valid with some different wording and the rest is word for word sims are pretty easy .
-  Thank you for the very helpful informations!
-  This dumps is enough to pass the exam and I have to do.

<http://www.gratisexam.com/>

## **Exam A**

### **QUESTION 1**

Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

- A. Vulnerability Assessment and Penetration Testing
- B. Security Certification and Accreditation (C&A)
- C. Change and Configuration Control
- D. Risk Adjustments

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 2**

Which of the following can be prevented by an organization using job rotation and separation of duties policies?

- A. Collusion
- B. Eavesdropping
- C. Buffer overflow
- D. Phishing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

Build Your Dreams

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation? Each correct answer represents a complete solution. Choose all that apply.

- A. Names of the victims
- B. Location of each incident
- C. Nature of harassment
- D. Date and time of incident

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 4

Which of the following types of evidence is considered as the best evidence?



<http://www.gratisexam.com/>

- A. A copy of the original document
- B. Information gathered through the witness's senses
- C. The original document

D. A computer-generated record

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

### **QUESTION 5**

What are the purposes of audit records on an information system? Each correct answer

represents a complete solution. Choose two.

- A. Troubleshooting
- B. Investigation
- C. Upgradation
- D. Backup

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 6**

Which of the following refers to an information security document that is used in the United

States Department of Defense (DoD) to describe and accredit networks and systems?

- A. SSAA
- B. FITSAF
- C. FIPS
- D. TCSEC

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is corrected.

**QUESTION 7**

Build Your Dreams

Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

- A. Vulnerability analysis
- B. Cost-benefit analysis
- C. Gap analysis
- D. Requirement analysis

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 8**

A contract cannot have provisions for which one of the following?

- A. Subcontracting the work
- B. Penalties and fines for disclosure of intellectual rights
- C. A deadline for the completion of the work
- D. Illegal activities

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 9**

Your company is covered under a liability insurance policy, which provides various liability

coverage for information security risks, including any physical damage of assets, hacking



<http://www.gratisexam.com/>

attacks, etc. Which of the following risk management techniques is your company using?

Build Your Dreams

- A. Risk mitigation
- B. Risk transfer
- C. Risk acceptance
- D. Risk avoidance

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 10**

You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. One of the employees of your organization asks you the purpose of the security awareness, training and education program. What will be your answer?

- A. It improves the possibility for career advancement of the IT staff.
- B. It improves the security of vendor relations.
- C. It improves the performance of a company's intranet.
- D. It improves awareness of the need to protect system resources.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this

Build Your Dreams  
called?

- A. Availability
- B. Encryption
- C. Integrity
- D. Confidentiality

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

- A. Scope Verification
- B. Project Management Information System
- C. Integrated Change Control
- D. Configuration Management System

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

Build Your Dreams

- A. Internet telephony
- B. Instant messaging
- C. Electronic mail
- D. Post-it note
- E. Blogs
- F. Internet teleconferencing

**Correct Answer:** ABCEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Answer: A, B, C, E, F

**QUESTION 14**

You are the project manager of the HJK project for your organization. You and the project team have created risk responses for many of the risk events in the project. A teaming agreement is an example of what risk response?

- A. Mitigation
- B. Sharing
- C. Acceptance
- D. Transference



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

Which of the following acts is a specialized privacy bill that affects any educational institution

Build Your Dreams

to accept any form of funding from the federal government?

- A. HIPAA
- B. COPPA
- C. FERPA
- D. GLBA

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

Which of the following steps is the initial step in developing an information security strategy?

- A. Perform a technical vulnerabilities assessment.
- B. Assess the current levels of security awareness.
- C. Perform a business impact analysis.
- D. Analyze the current business strategy.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is valid.

**QUESTION 17**

Which of the following statements about the integrity concept of information security

management are true? Each correct answer represents a complete solution. Choose three.

- A. It ensures that unauthorized modifications are not made to data by authorized personnel or Build Your Dreams processes.
- B. It determines the actions and behaviors of a single individual within a system
- C. It ensures that modifications are not made to data by unauthorized personnel or processes.
- D. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

Which of the following contract types is described in the statement below? "This contract type

provides no incentive for the contractor to control costs and hence is rarely utilized."

- A. Cost Plus Fixed Fee
- B. Cost Plus Percentage of Cost
- C. Cost Plus Incentive Fee
- D. Cost Plus Award Fee

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

Ned is the program manager for his organization and he's considering some new materials for

his program. He and his team have never worked with these materials before and he wants to

ask the vendor for some additional information, a demon, and even some samples. What type

Build Your Dreams

of a document should Ned send to the vendor?

- A. IFB
- B. RFQ
- C. RFP
- D. RFI

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 20**

Against which of the following does SSH provide protection? Each correct answer represents

a complete solution. Choose two.

- A. IP spoofing
- B. Broadcast storm
- C. Password sniffing
- D. DoS attack

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 21**

What is a stakeholder analysis chart?



<http://www.gratisexam.com/>

- A. It is a matrix that documents stakeholders' threats, perceived threats, and communication Build Your Dreams needs.
- B. It is a matrix that identifies all of the stakeholders and to whom they must report to.
- C. It is a matrix that documents the stakeholders' requirements, when the requirements were created, and when the fulfillment of the requirements took place..
- D. It is a matrix that identifies who must communicate with whom.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 22**

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

- A. Disaster Recovery Plan
- B. Continuity of Operations Plan
- C. Contingency Plan
- D. Business Continuity Plan

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

You are a project manager of a large construction project. Within the project you are working with several vendors to complete different phases of the construction. Your client has asked that you arrange for some of the materials a vendor is to install next week in the project to be changed. According to the change management plan what subsystem will need to manage

Build Your Dreams  
this change request?

- A. Cost
- B. Resources
- C. Contract
- D. Schedule

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

- A. The Configuration Manager
- B. The Supplier Manager
- C. The Service Catalogue Manager
- D. The IT Service Continuity Manager

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 25**

In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

Build Your Dreams

- A. Initiation Phase
- B. Development/Acquisition Phase
- C. Implementation Phase
- D. Operation/Maintenance Phase

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

- A. Malicious Communications Act (1998)
- B. Anti-Cyber-Stalking law (1999)
- C. Stalking Amendment Act (1999)
- D. Stalking by Electronic Communications Act (2001)

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

Which of the following response teams aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large?

Build Your Dreams

- A. CSIRT
- B. CERT
- C. FIRST
- D. FedCIRC

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 28**

Which of the following statements is related with the first law of OPSEC?

- A. If you are not protecting it (the critical and sensitive information), the adversary wins!
- B. If you don't know what to protect, how do you know you are protecting it?
- C. If you don't know about your security resources you could not protect your network.
- D. If you don't know the threat, how do you know what to protect?

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 29**

Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. Who decides the category of a change?

- A. The Problem Manager
- B. The Process Manager
- C. The Change Manager  
Build Your Dreams
- D. The Service Desk
- E. The Change Advisory Board

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Direct
- B. Circumstantial
- C. Incontrovertible
- D. Corroborating

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?



- A. PROTECT Act
- B. Sexual Predators Act  
Build Your Dreams
- C. Civil Rights Act of 1991
- D. The USA Patriot Act of 2001

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is modified.

**QUESTION 32**

Which of the following policies helps reduce the potential damage from the actions of one person?

- A. CSA
- B. Risk assessment
- C. Separation of duties
- D. Internal audit

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes. Which of the following are Change Management



<http://www.gratisexam.com/>

terminologies? Each correct answer represents a part of the solution. Choose three.

- A. Request for Change
- B. Service Request Management
- C. Change  
Build Your Dreams
- D. Forward Schedule of Changes

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 34**

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Initial analysis, request for service, data collection, data reporting, data analysis
- B. Initial analysis, request for service, data collection, data analysis, data reporting
- C. Request for service, initial analysis, data collection, data analysis, data reporting
- D. Request for service, initial analysis, data collection, data reporting, data analysis

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?

- A. The Service Level Manager
  - B. The Configuration Manager
  - C. The IT Security Manager
  - D. The Change Manager
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

James works as a security manager for SoftTech Inc. He has been working on the continuous process improvement and on the ordinal scale for measuring the maturity of the organization involved in the software processes. According to James, which of the following maturity levels of software CMM focuses on the continuous process improvement?

- A. Repeatable level
- B. Defined level
- C. Initiating level
- D. Optimizing level

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

- A. Patent
  - B. Utility model
  - C. Snooping
  - D. Copyright
- Build Your Dreams

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

- A. Cold site
- B. Off site
- C. Hot site
- D. Warm site

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

Which of the following is a process of monitoring data packets that travel across a network?

- A. Password guessing
- B. Packet sniffing
- C. Shielding
- D. Packet filtering

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 40**

Mark works as a security manager for SofTech Inc. He is working in a partially equipped office space which contains some of the system hardware, software, telecommunications, and power sources. In which of the following types of office sites is he working?

- A. Mobile site
- B. Warm site
- C. Cold site
- D. Hot site

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 41**

You are documenting your organization's change control procedures for project management.

What portion of the change control process oversees features and functions of the product scope?

- A. Configuration management

- B. Product scope management is outside the concerns of the project.
- C. Scope change control system
- D. Project integration management

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 42**

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

- A. Spam
- B. Patent
- C. Artistic license
- D. Phishing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 43**

Which of the following are the major tasks of risk management? Each correct answer represents a complete solution. Choose two.

- A. Assuring the integrity of organizational data
- B. Building Risk free systems
- C. Risk control
- D. Risk identification

**Correct Answer:** CD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

Build Your Dreams

Which of the following statements best describes the consequences of the disaster recovery

plan test?

- A. If no deficiencies were found during the test, then the test was probably flawed.
- B. The plan should not be changed no matter what the results of the test would be.
- C. The results of the test should be kept secret.
- D. If no deficiencies were found during the test, then the plan is probably perfect.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

well modified.

**QUESTION 45**

Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP) ?

- A. UDP port 161
- B. TCP port 443
- C. TCP port 110
- D. UDP port 1701

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

Build Your Dreams

- A. Provide diligent and competent service to principals.
- B. Protect society, the commonwealth, and the infrastructure.
- C. Give guidance for resolving good versus good and bad versus bad dilemmas.
- D. Act honorably, honestly, justly, responsibly, and legally.

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 47**

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

- A. Performing quality control
- B. Recreating and analyzing the problem
- C. Developing the changes and corresponding tests
- D. Establishing the priorities of requests

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

Which of the following statements about Due Care policy is true?



- A. It is a method used to authenticate users on a network.
- B. It is a method for securing database servers.  
Build Your Dreams
- C. It identifies the level of confidentiality of information.
- D. It provides information about new viruses.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 49**

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

- A. Configuration Verification and Auditing
- B. Configuration Item Costing
- C. Configuration Identification
- D. Configuration Status Accounting

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 50**

What are the steps related to the vulnerability management program? Each correct answer represents a complete solution. Choose all that apply.

- A. Maintain and Monitor  
Build Your Dreams
- B. Organization Vulnerability
- C. Define Policy
- D. Baseline the Environment

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 51**

Which of the following is a documentation of guidelines that are used to create archival copies of important data?

- A. User policy
- B. Security policy
- C. Audit policy
- D. Backup policy

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 52**

Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

- A. Outsource
- B. Proposal
- C. Contract  
Build Your Dreams

D. Service level agreement

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)
- D. Annualized Rate of Occurrence (ARO)

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

Which of the following types of agreement creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret?

- A. SLA
  - B. NDA
  - C. Non-price competition
  - D. CNC
- Build Your Dreams

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 55**

Which of the following sections come under the ISO/IEC 27002 standard?

- A. Financial assessment
- B. Asset management
- C. Security policy
- D. Risk assessment

**Correct Answer:** BCD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56**

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.C. 1362
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 1029
- D. 18 U.S.C. 2701
- E. 18 U.S.C. 2510

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 57**

Which of the following access control models uses a predefined set of access privileges for



<http://www.gratisexam.com/>

an object of a system?

- A. Role-Based Access Control
- B. Mandatory Access Control
- C. Policy Access Control
- D. Discretionary Access Control

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

Which of the following statements about the availability concept of Information security

management is true?

- A. It determines actions and behaviors of a single individual within a system.
- B. It ensures reliable and timely access to resources.
- C. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
- D. It ensures that modifications are not made to data by unauthorized personnel or processes.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 59**

Which of the following is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems?

- A. IDS
- B. OPSEC
- C. HIDS
- D. NIDS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

Which of the following administrative policy controls is usually associated with government classifications of materials and the clearances of individuals to access those materials?

- A. Separation of Duties
- B. Due Care
- C. Acceptable Use
- D. Need to Know

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

Which of the following processes will you involve to perform the active analysis of the system

Build Your Dreams  
for any potential vulnerabilities that may result from poor or improper system configuration,

known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

- A. Penetration testing
- B. Risk analysis
- C. Baselineing
- D. Compliance checking

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 62**

Which of the following are the levels of military data classification system? Each correct answer represents a complete solution. Choose all that apply.

- A. Sensitive
- B. Top Secret
- C. Confidential
- D. Secret
- E. Unclassified
- F. Public

**Correct Answer:** ABCDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Answer: A, B, C, D, E

Build Your Dreams

#### **QUESTION 63**

Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

- A. Device Seizure
- B. Ontrack
- C. DriveSpy
- D. Forensic Sorter

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 64**

Which of the following needs to be documented to preserve evidences for presentation in court?

- A. Separation of duties
- B. Account lockout policy
- C. Incident response policy
- D. Chain of custody

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 65**

Which of the following statements best explains how encryption works on the Internet?

Build Your Dreams

- A. Encryption encodes information using specific algorithms with a string of numbers known as a key.



- B. Encryption validates a username and password before sending information to the Web server.
- C. Encryption allows authorized users to access Web sites that offer online shopping.
- D. Encryption helps in transaction processing by e-commerce servers on the Internet.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 66**

Which of the following statutes is enacted in the U.S., which prohibits creditors from collecting data from applicants, such as national origin, caste, religion etc?

- A. The Fair Credit Reporting Act (FCRA)
- B. The Privacy Act
- C. The Electronic Communications Privacy Act
- D. The Equal Credit Opportunity Act (ECOA)

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 67**

Which of the following security models deal only with integrity? Each correct answer represents a complete solution. Choose two.

Build Your Dreams

- A. Biba-Wilson
- B. Clark-Wilson
- C. Bell-LaPadula
- D. Biba

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

Rick is the project manager for TTM project. He is in the process of procuring services from vendors. He makes a contract with a vendor in which he precisely specify the services to be procured, and any changes to the procurement specification will increase the costs to the buyer. Which type of contract is this?

- A. Firm Fixed Price
- B. Fixed Price Incentive Fee
- C. Cost Plus Fixed Fee Contract
- D. Fixed Price with Economic Price Adjustment

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires Build Your Dreams different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

- A. Preparation

- B. Eradication
- C. Identification
- D. Containment

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 70**

Which of the following security models focuses on data confidentiality and controlled access

to classified information?

- A. Bell-La Padula model
- B. Take-Grant model
- C. Clark-Wilson model
- D. Biba model

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 71**

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or



<http://www.gratisexam.com/>

state of affairs?

- A. Disaster recovery plan
- B. Contingency plan
- C. Continuity of Operations Plan
- D. Business continuity plan

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 72**

Which of the following BCP teams handles financial arrangement, public relations, and media

inquiries in the time of disaster recovery?

- A. Software team
- B. Off-site storage team
- C. Applications team
- D. Emergency-management team

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

- A. Yes, the ZAS Corporation did not choose to terminate the contract work.
  - B. It depends on what the outcome of a lawsuit will determine.
  - C. It depends on what the termination clause of the contract stipulates.
  - D. No, the ZAS Corporation did not complete all of the work.
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 74**

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Assessing the impact of potential threats
- B. Identifying the accused
- C. Finding an economic balance between the impact of the risk and the cost of the countermeasure
- D. Identifying the risk

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 75**

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

- A. Quantitative risk analysis
  - B. Qualitative risk analysis
  - C. Requested changes
  - D. Risk audits
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 76**

Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question? Each correct answer represents a part of the solution. Choose three.

- A. Protect an organization from major computer services failure.
- B. Minimize the risk to the organization from delays in providing services.
- C. Guarantee the reliability of standby systems through testing and simulation.
- D. Maximize the decision-making required by personnel during a disaster.

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

- A. Programming and training
- B. Evaluation and acceptance
- C. Definition
- D. Initiation

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?

- A. Identification information for each stakeholder
- B. Assessment information of the stakeholders' major requirements, expectations, and potential influence

Build Your Dreams

- C. Stakeholder classification of their role in the project
- D. Stakeholder management strategy

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 79**

Which of the following are examples of physical controls used to prevent unauthorized access

to sensitive materials?

- A. Thermal alarm systems
- B. Closed circuit cameras
- C. Encryption
- D. Security Guards

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 80**

Which of the following security issues does the Bell-La Padula model focus on?

- A. Authentication
  - B. Confidentiality
  - C. Integrity
  - D. Authorization
- Build Your Dreams

**Correct Answer:** B

**Section:** (none)



**Explanation****Explanation/Reference:****QUESTION 81**

Which of the following are the examples of administrative controls? Each correct answer represents a complete solution. Choose all that apply.

- A. Security awareness training
- B. Security policy
- C. Data Backup
- D. Auditing

**Correct Answer:** AB

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 82**

Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

- A. Administrative
- B. Automatic
- C. Physical
- D. Technical

**Correct Answer:** ACD

**Section:** (none)

**Explanation****Explanation/Reference:**

Build Your Dreams

**QUESTION 83**

Which of the following laws enacted in United States makes it illegal for an Internet Service

Provider (ISP) to allow child pornography to exist on Web sites?

- A. Child Pornography Prevention Act (CPPA)
- B. USA PATRIOT Act
- C. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
- D. Sexual Predators Act

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is perfected.

#### **QUESTION 84**

Which of the following representatives of incident response team takes forensic backups of

the systems that are the focus of the incident?

- A. Legal representative
- B. Technical representative
- C. Lead investigator
- D. Information security representative

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 85**

Build Your Dreams

A Web-based credit card company had collected financial and personal details of Mark before

issuing him a credit card. The company has now provided Mark's financial and personal

details to another company. Which of the following Internet laws has the credit card issuing

company violated?

- A. Copyright law
- B. Trademark law
- C. Privacy law
- D. Security law

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 86**

You work as a Web Administrator for Perfect World Inc. The company is planning to host an E-commerce Web site. You are required to design a security plan for it. Client computers with different operating systems will access the Web server. How will you configure the Web server so that it is secure and only authenticated users are able to access it? Each correct answer represents a part of the solution. Choose two.

- A. Use encrypted authentication.
  - B. Use the SSL protocol.
  - C. Use the EAP protocol.
  - D. Use Basic authentication.
- Build Your Dreams

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 87**

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

- A. They can be analyzed and measured by the risk analysis process.
- B. They can be removed completely by taking proper actions.
- C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
- D. They are considered an indicator of threats coupled with vulnerability.

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 88**

Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

- A. Organizational chart reviews
- B. Executive management interviews
- C. Overlaying system technology
- D. Organizational process models

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 89**

Which of the following BCP teams provides clerical support to the other teams and serves as a message center for the user-recovery site?

- A. Security team

- B. Data preparation and records team
- C. Administrative support team
- D. Emergency operations team

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 90**

Which of the following architecturally related vulnerabilities is a hardware or software mechanism, which was installed to permit system maintenance and to bypass the system's security protections?

- A. Maintenance hook
- B. Lack of parameter checking
- C. Time of Check to Time of Use (TOC/TOU) attack
- D. Covert channel

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 91**

You have created a team of HR Managers and Project Managers for Blue Well Inc. The team will concentrate on hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. Which of the following steps will you perform to accomplish the task?

- A. Job rotation

- B. Job responsibility
- C. Screening candidates
- D. Separation of duties

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 92**

Your project has several risks that may cause serious financial impact should they happen.

You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

- A. Quantitative analysis
- B. Contingency reserve
- C. Risk response  
Build Your Dreams
- D. Risk response plan

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 93**

Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

- A. Data custodian
- B. Auditor
- C. User
- D. Data owner

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 94**

Which of the following are the process steps of OPSEC? Each correct answer represents a part of the solution. Choose all that apply.

- A. Analysis of Vulnerabilities
  - B. Display of associated vulnerability components
  - C. Assessment of Risk
  - D. Identification of Critical Information
- Build Your Dreams

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 95**

You work as a project manager for SoftTech Inc. A threat with a dollar value of \$150,000 is expected to happen in your project and the frequency of threat occurrence per year is 0.001.

What will be the annualized loss expectancy in your project?

- A. \$180.25
- B. \$150

- C. \$100
- D. \$120

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 96**

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution.

Choose three.

- A. Determining what level of classification the information requires.
  - B. Delegating the responsibility of the data protection duties to a custodian.
  - C. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.
  - D. Running regular backups and routinely testing the validity of the backup data.
- Build Your Dreams

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 97**

You work as the Network Administrator for a defense contractor. Your company works with sensitive materials and all IT personnel have at least a secret level clearance. You are still





<http://www.gratisexam.com/>

concerned that one individual could perhaps compromise the network (intentionally or unintentionally) by setting up improper or unauthorized remote access. What is the best way to avoid this problem?

- A. Implement separation of duties.
- B. Implement RBAC.
- C. Implement three way authentication.
- D. Implement least privileges.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 98**

Which of the following statements is true about auditing?

- A. It is used to protect the network against virus attacks.
  - B. It is used to track user accounts for file and object access, logon attempts, etc.
  - C. It is used to secure the network or the computers on the network.
  - D. It is used to prevent unauthorized access to network resources.
- Build Your Dreams

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99**

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

- A. Earned value management
- B. Risk audit
- C. Technical performance measurement
- D. Corrective action

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 100**

Mark works as a security manager for SoftTech Inc. He is performing a security awareness program. To be successful in performing the awareness program, he should take into account the needs and current levels of training and understanding of the employees and audience. There are five key ways, which Mark should keep in mind while performing this activity. Current level of computer usage What the audience really wants to learn How receptive the audience is to the security program How to gain acceptance Who might be a possible ally Which of the following activities is performed in this security awareness process?

- A. Separation of duties
- B. Stunned owl syndrome
- C. Audience participation
- D. Audience segmentation

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 101**

Rachael is the project manager for a large project in her organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can Rachael do in this instance?

Build Your Dreams

- A. Threaten to sue the vendor if they don't complete the work.
- B. Fire the vendor for failing to complete the contractual obligation.
- C. Withhold the vendor's payments for the work they've completed.
- D. Refer to the contract agreement for direction.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 102**

How many change control systems are there in project management?

- A. 3
- B. 4
- C. 2
- D. 1

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 103**

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

- A. Programming and training
- B. Evaluation and acceptance  
Build Your Dreams
- C. Initiation
- D. Design

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 104**

Which of the following signatures watches for the connection attempts to well-known, frequently attacked ports?

- A. Port signatures
- B. Digital signatures

- C. Header condition signatures
- D. String signatures

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 105**

Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. Configuration Management is used for which of the following? 1.To account for all IT assets 2.To provide precise information support to other ITIL disciplines 3.To provide a solid base only for Incident and Problem Management 4.To verify configuration records and correct any exceptions

- A. 1, 3, and 4 only  
Build Your Dreams
- B. 2 and 4 only
- C. 1, 2, and 4 only
- D. 2, 3, and 4 only

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 106**

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

- A. TLS
- B. HTTP
- C. SNMP
- D. SSL

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 107**

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

- A. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
- B. Asset Value X Exposure Factor (EF)  
Build Your Dreams
- C. Exposure Factor (EF)/Single Loss Expectancy (SLE)
- D. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 108**

Which of the following rate systems of the Orange book has no security controls?

- A. D-rated
- B. C-rated
- C. E-rated
- D. A-rated

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 109**

Which of the following documents is described in the statement below? "It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

- A. Risk register
  - B. Risk management plan
  - C. Quality management plan
  - D. Project charter
- Build Your Dreams

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 110**

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

- A. PAP
- B. EAP
- C. MS-CHAP v2
- D. CHAP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 111**

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

- A. Penetration testing
- B. On-site interviews
- C. Security Test and Evaluation (ST&E)
- D. Automated vulnerability scanning tool

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 112**

Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

- A. Strict adherence to this Code is a condition of certification.
- B. Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- C. Advance and protect the profession.
- D. Provide diligent and competent service to principals.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 113**



Which of the following options is an approach to restricting system access to authorized users?

- A. DAC
- B. MIC
- C. RBAC
- D. MAC

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 114**

You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of \_\_\_\_.

- A. Conflict of interest
- B. Bribery
- C. Illegal practice
- D. Irresponsible practice

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 115**

What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

- A. ZOPA
- B. PON
- C. Bias
- D. BATNA

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 116**

Build Your Dreams

Which of the following terms describes a repudiation of a contract that occurs before the time when performance is due?

- A. Expected breach
- B. Actual breach
- C. Anticipatory breach
- D. Nonperforming breach

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 117**

Which of the following is generally practiced by the police or any other recognized governmental authority?

- A. Phishing
- B. Wiretapping
- C. SMB signing
- D. Spoofing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 118**

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

Build Your Dreams

- A. Evidence access policy
- B. Incident response policy
- C. Chain of custody
- D. Chain of evidence

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 119**

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)
- D. Annualized Rate of Occurrence (ARO)

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

Which of the following statements is related with the second law of OPSEC?

- A. If you are not protecting it (the critical and sensitive information), the adversary wins!
- B. If you don't know what to protect, how do you know you are protecting it? Build Your Dreams
- C. If you don't know about your security resources you could not protect your network.
- D. If you don't know the threat, how do you know what to protect?

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 121**

Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

- A. Business continuity plan development
- B. Business impact assessment
- C. Scope and plan initiation
- D. Plan approval and implementation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

Which of the following Acts enacted in United States allows the FBI to issue National Security

Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

- A. Electronic Communications Privacy Act of 1986
- B. Wiretap Act
- C. Computer Fraud and Abuse Act
- D. Economic Espionage Act of 1996

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 123**

You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project? Each correct answer represents a complete solution. Choose all that apply.

- A. It provides object, orient, decide and act strategy.
  - B. It provides a live documentation of the project.
  - C. It provides the risk analysis of project configurations.
  - D. It provides the versions for network devices.
- Build Your Dreams

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 124**

You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step for you to take in preserving the chain of custody?

- A. Preserve the email server including all logs.
- B. Seize the employee's PC.
- C. Make copies of that employee's email.
- D. Place spyware on the employee's PC to confirm these activities.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 125**

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

- A. Secret
- B. Sensitive
- C. Unclassified
- D. Private
- E. Confidential
- F. Public

**Correct Answer:** BDEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 126**

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain



<http://www.gratisexam.com/>

an economic advantage over its competitors?

- A. Utility model
- B. Cookie
- C. Copyright
- D. Trade secret

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 127**

Which of the following backup sites takes the longest recovery time?

- A. Cold site
  - B. Hot site
  - C. Warm site
  - D. Mobile backup site
- Build Your Dreams

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 128**

John works as a security manager for Soft Tech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Full-scale exercise
- B. Walk-through drill
- C. Evacuation drill
- D. Structured walk-through test

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 129**

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

- A. Information dissemination policy
- B. Electronic monitoring statement  
Build Your Dreams
- C. Additional personnel security controls



D. Incident response plan

**Correct Answer:** ABCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 130**

Which of the following attacks can be mitigated by providing proper training to the employees in an organization?

- A. Social engineering
- B. Smurf
- C. Denial-of-Service
- D. Man-in-the-middle

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

Which of the following is the default port for Simple Network Management Protocol (SNMP)?

- A. TCP port 80
  - B. TCP port 25
  - C. UDP port 161
  - D. TCP port 110
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 132**

Which of the following is a variant with regard to Configuration Management?

- A. A CI that has the same name as another CI but shares no relationship.
- B. A CI that particularly refers to a hardware specification.
- C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
- D. A CI that particularly refers to a software version.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 133**

You work as a Forensic Investigator. Which of the following rules will you follow while working on a case? Each correct answer represents a part of the solution. Choose all that apply.

- A. Prepare a chain of custody and handle the evidence carefully.
- B. Examine original evidence and never rely on the duplicate evidence.
- C. Never exceed the knowledge base of the forensic investigation.
- D. Follow the rules of evidence and never temper with the evidence.

**Correct Answer:** ABCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 134**

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution.

Choose three.

- A. Determining what level of classification the information requires
- B. Running regular backups and routinely testing the validity of the backup data
- C. Controlling access, adding and removing privileges for individual users
- D. Performing data restoration from the backups when necessary

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 135**

Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are

true? Each correct answer represents a complete solution. Choose two.

- A. It uses TCP port 80 as the default port.
- B. It is a protocol used in the Universal Resource Locator (URL) address line to connect to a secure site.
- C. It uses TCP port 443 as the default port.
- D. It is a protocol used to provide security for a database server in an internal network.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 136**

John is a black hat hacker. FBI arrested him while performing some email scams. Under

which of the following US laws will john be charged?

- A. 18 U.S.C. 1362
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 2701

D. 18 U.S.C. 2510

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 137**

Which of the following statements are true about a hot site? Each correct answer represents a complete solution. Choose all that apply.

- A. It can be used within an hour for data recovery.
- B. It is cheaper than a cold site but more expensive than a warm site.
- C. It is the most inexpensive backup site.
- D. It is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 138**

Build Your Dreams

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. Which of the following are some of its critical steps? Each correct answer represents a complete solution. Choose two.

- A. Awareness and Training Material Effectiveness
- B. Awareness and Training Material Development
- C. Awareness and Training Material Implementation

D. Awareness and Training Program Design

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 139**

You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

- A. Cost plus incentive fee
- B. Fixed fee
- C. Cost plus percentage of costs
- D. Time and materials

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 140**

You are the Network Administrator for a college. You watch a large number of people (some not even students) going in and out of areas with campus computers (libraries, computer labs, etc.). You have had a problem with laptops being stolen. What is the most cost effective method to prevent this?

- A. Video surveillance on all areas with computers.

- B. Use laptop locks.
- C. Appoint a security guard.
- D. Smart card access to all areas with computers.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

up-to-date.

#### **QUESTION 141**

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Availability
  - B. Confidentiality
  - C. Integrity
  - D. Authenticity
- Build Your Dreams

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 142**

Which of the following plans provides procedures for recovering business operations immediately following a disaster?

- A. Disaster recovery plan
- B. Business continuity plan
- C. Continuity of operation plan
- D. Business recovery plan

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 143**

In which of the following contract types, the seller is reimbursed for all allowable costs for performing the contract work and receives a fixed fee payment which is calculated as a percentage of the initial estimated project costs?

- A. Firm Fixed Price Contracts
- B. Cost Plus Fixed Fee Contracts
- C. Fixed Price Incentive Fee Contracts
- D. Cost Plus Incentive Fee Contracts  
Build Your Dreams

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 144**

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

- A. Encouraging others to harass the victim
- B. False accusations
- C. Attempts to gather information about the victim
- D. False victimization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 145**

Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

- A. Risk management
  - B. Configuration management
  - C. Change management
  - D. Procurement management
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 146**

Mark is the project manager of the NHQ project in Spartech Inc. The project has an asset valued at \$195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

- A. \$92,600
- B. \$67,250



- C. \$68,250
- D. \$72,650

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 147**

Which of the following is the default port for Secure Shell (SSH)?

- A. UDP port 161
- B. TCP port 22
- C. UDP port 138
- D. TCP port 443

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

#### **QUESTION 148**

Which of the following is used to back up forensic evidences or data folders from the network

or locally attached hard disk drives?

- A. WinHex
- B. Vedit
- C. Device Seizure
- D. FAR system

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 149**

You work as a security manager for SoftTech Inc. You along with your team are doing the disaster recovery for your project. Which of the following steps are performed by you for secure recovery based on the extent of the disaster and the organization's recovery ability?

Each correct answer represents a part of the solution. Choose three.

- A. Recover to an alternate site for critical functions
- B. Restore full system at an alternate operating site
- C. Restore full system after a catastrophic loss
- D. Recover at the primary operating site

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 150**

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

- A. System Definition
- B. Accreditation
- C. Verification
- D. Re-Accreditation
- E. Validation
- F. Identification

**Correct Answer:** ACDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 151**

Management has asked you to perform a risk audit and report back on the results. Bonny, a project team member asks you what a risk audit is. What do you tell Bonny?

- A. A risk audit is a review of all the risks that have yet to occur and what their probability of happening are.
- B. A risk audit is a review of the effectiveness of the risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management process.  
Build Your Dreams
- C. A risk audit is a review of all the risk probability and impact for the risks, which are still present in the project but which have not yet occurred.
- D. A risk audit is an audit of all the risks that have occurred in the project and what their true impact on cost and time has been.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 152**

Which of the following steps are generally followed in computer forensic examinations? Each correct answer represents a complete solution. Choose three.

- A. Acquire
- B. Analyze
- C. Authenticate
- D. Encrypt

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 153**

Which of the following methods can be helpful to eliminate social engineering threat? Each



<http://www.gratisexam.com/>

correct answer represents a complete solution. Choose three.

- A. Password policies
- B. Vulnerability assessments  
Build Your Dreams
- C. Data encryption
- D. Data classification

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 154**

You work as a security manager for SoftTech Inc. You are conducting a security awareness

campaign for your employees. Which of the following ideas will you consider the best when

conducting a security awareness campaign?

- A. Target system administrators and the help desk.
- B. Provide technical details on exploits.
- C. Provide customized messages for different groups.

D. Target senior managers and business process owners.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 155**

Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

- A. Second Code of Ethics Canons
- B. Fourth Code of Ethics Canons
- C. First Code of Ethics Canons  
Build Your Dreams
- D. Third Code of Ethics Canons

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 156**

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

- A. B-rated
- B. C-rated
- C. D-rated
- D. A-rated

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 157**

Which of the following SDLC phases consists of the given security controls. Misuse Case

Modeling Security Design and Architecture Review Threat and Risk Modeling Security

Requirements and Test Cases Generation

- A. Design
- B. Maintenance
- C. Deployment
- D. Requirements Gathering  
Build Your Dreams

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 158**

Which of the following liabilities is a third-party liability in which an individual may be

responsible for an action by another party?

- A. Relational liability
- B. Engaged liability
- C. Contributory liability
- D. Vicarious liability

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 159**

Which of the following measurements of an enterprise's security state is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results?

- A. Information sharing
  - B. Ethics
  - C. Performance measurement
  - D. Risk management
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 160**

You are the Network Administrator for a software company. Due to the nature of your company's business, you have a significant number of highly computer savvy users. However, you have still decided to limit each user access to only those resources required for their job, rather than give wider access to the technical users (such as tech support and software engineering personnel). What is this an example of?

- A. The principle of maximum control.
- B. The principle of least privileges.
- C. Proper use of an ACL.
- D. Poor resource management.

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 161**

Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

- A. Employee registration and accounting
- B. Disaster preparedness and recovery plans
- C. Network authentication  
Build Your Dreams
- D. Training and awareness
- E. Encryption

**Correct Answer:** ABD

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 162**

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. NSA-IAM
- B. DITSCAP
- C. ASSET
- D. NIACAP

**Correct Answer:** D



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 163**

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee  
Build Your Dreams
- D. Chief Information Security Officer

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 164**

Which of the following divisions of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy?

- A. Division A
- B. Division D
- C. Division B
- D. Division C

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 165**

Which of the following sites are similar to the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities?

- A. Cold sites
- B. Orange sites
- C. Warm sites
- D. Duplicate processing facilities  
Build Your Dreams

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 166**

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

- A. Disaster Recovery Plan
- B. Contingency Plan
- C. Continuity Of Operations Plan
- D. Business Continuity Plan

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 167**

Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

- A. Communications management plan
- B. Change management plan
- C. Issue log  
Build Your Dreams
- D. Risk management plan

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 168**

Which of the following laws is defined as the Law of Nations or the legal norms that has developed through the customary exchanges between states over time, whether based on diplomacy or aggression?

- A. Customary
- B. Tort
- C. Criminal
- D. Administrative

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 169**

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

- A. Availability
  - B. Non-repudiation
  - C. Integrity
  - D. Confidentiality
- Build Your Dreams

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 170**

Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

- A. Internet Crimes Against Children (ICAC)
- B. Project Safe Childhood (PSC)
- C. Anti-Child Porn.org
- D. Innocent Images National Initiative (IINI)

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 171**

You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the risk events. You and the

project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

- A. Risk mitigation
- B. Risk acceptance
- C. Risk avoidance  
Build Your Dreams
- D. Risk transference

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 172**

Which of the following are known as the three laws of OPSEC? Each correct answer represents a part of the solution. Choose three.

- A. If you don't know the threat, how do you know what to protect?
- B. If you don't know what to protect, how do you know you are protecting it?
- C. If you are not protecting it (the critical and sensitive information), the adversary wins!
- D. If you don't know about your security resources you cannot protect your network.

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 173**

Build Your Dreams

In which of the following alternative processing sites is the backup facility maintained in a

constant order, with a full complement of servers, workstations, and communication links

ready to assume the primary operations responsibility?

- A. Mobile Site
- B. Cold Site
- C. Warm Site
- D. Hot Site

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 174**

Which of the following processes is used by remote users to make a secure connection to

internal resources after establishing an Internet connection?

- A. Packet filtering
- B. Tunneling
- C. Packet sniffing
- D. Spoofing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 175**

Which of the following is a name, symbol, or slogan with which a product is identified?

Build Your Dreams

- A. Copyright
- B. Trademark
- C. Trade secret
- D. Patent

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 176**

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

- A. Network security policy
- B. Backup policy
- C. Privacy policy
- D. User password policy

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 177**

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

- A. No  
Build Your Dreams
- B. Yes

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 178**

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

- A. Take-Grant Protection Model
- B. Bell-LaPadula Model
- C. Biba Integrity Model
- D. Access Matrix

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 179**

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of



<http://www.gratisexam.com/>

normal business processes?

- A. Business continuity plan
- B. Crisis communication plan



- C. Contingency plan
  - D. Disaster recovery plan
- Build Your Dreams

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 180**

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Privacy

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 181**

Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

- A. Shielding
- B. Spoofing
- C. Eavesdropping
- D. Packaging

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 182**

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation.

Which of the following procedures will you employ to accomplish the task?

- A. Configuration identification
- B. Physical configuration audit
- C. Configuration control
- D. Functional configuration audit

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 183**

In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

- A. Role-Based Access Control
  - B. Discretionary Access Control
  - C. Task-based Access Control
  - D. Mandatory Access Control
- Build Your Dreams

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 184**

Which of the following access control models are used in the commercial sector? Each

correct answer represents a complete solution. Choose two.

- A. Clark-Biba model
- B. Clark-Wilson model
- C. Bell-LaPadula model
- D. Biba model

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 185**

Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems?

- A. Gramm-Leach-Bliley Act
- B. Computer Fraud and Abuse Act
- C. Computer Security Act
- D. Digital Millennium Copyright Act

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 186**

Which of the following security models deal only with integrity? Each correct answer represents a complete solution. Choose two.

- A. Biba-Wilson
- B. Clark-Wilson
- C. Bell-LaPadula
- D. Biba

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 187**

Rick is the project manager for TTM project. He is in the process of procuring services from vendors. He makes a contract with a vendor in which he precisely specify the services to be procured, and any changes to the procurement specification will increase the costs to the buyer. Which type of contract is this?

- A. Firm Fixed Price
- B. Fixed Price Incentive Fee
- C. Cost Plus Fixed Fee Contract
- D. Fixed Price with Economic Price Adjustment

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 188**

Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

- A. Yes, the ZAS Corporation did not choose to terminate the contract work.
- B. It depends on what the outcome of a lawsuit will determine.

- C. It depends on what the termination clause of the contract stipulates.
- D. No, the ZAS Corporation did not complete all of the work.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 189**

Which of the following are the process steps of OPSEC? Each correct answer represents a part of the solution. Choose all that apply.

- A. Analysis of Vulnerabilities
- B. Display of associated vulnerability components
- C. Assessment of Risk
- D. Identification of Critical Information

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 190**

Which of the following is generally practiced by the police or any other recognized governmental authority?

- A. Phishing
- B. Wiretapping
- C. SMB signing
- D. Spoofing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 191**

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

- A. Disaster Recovery Plan
- B. Contingency Plan
- C. Continuity Of Operations Plan
- D. Business Continuity Plan

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 192**

Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

- A. Configuration management
- B. Risk management
- C. Procurement management
- D. Change management

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 193**

Which of the following are the ways of sending secure e-mail messages over the Internet?

Each correct answer represents a complete solution. Choose two.

- A. TLS
- B. PGP
- C. S/MIME
- D. IPSec

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 194**

You work as a Senior Marketing Manager for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident. Which of the following steps of an incident handling process was performed by the incident response team?

- A. Containment
- B. Eradication
- C. Preparation
- D. Identification

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 195**

Which of the following is the process performed between organizations that have unique

hardware or software that cannot be maintained at a hot or warm site?

Build Your Dreams

- A. Cold sites arrangement
- B. Business impact analysis
- C. Duplicate processing facilities
- D. Reciprocal agreements

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 196**

Which of the following involves changing data prior to or during input to a computer in an

effort to commit fraud?

- A. Data diddling
- B. Wiretapping
- C. Eavesdropping
- D. Spoofing

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 197**

Which of the following penetration testing phases involves reconnaissance or data gathering?

- A. Attack phase
- B. Pre-attack phase  
Build Your Dreams
- C. Post-attack phase
- D. Out-attack phase

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 198**

Mark works as a security manager for SoftTech Inc. He is involved in the BIA phase to create a document to be used to help understand what impact a disruptive event would have on the business. The impact might be financial or operational. Which of the following are the objectives related to the above phase in which Mark is involved? Each correct answer represents a part of the solution. Choose three.

- A. Resource requirements identification
- B. Criticality prioritization
- C. Down-time estimation
- D. Performing vulnerability assessment

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 199**

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

Build Your Dreams

- A. Business continuity plan
- B. Disaster recovery plan
- C. Continuity of Operations Plan
- D. Contingency plan

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 200**

Which of the following protocols is used with a tunneling protocol to provide security?

- A. FTP
- B. IPX/SPX
- C. IPSec
- D. EAP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 201**

Which of the following subphases are defined in the maintenance phase of the life cycle

models?

- A. Change control
- B. Configuration control
- C. Request control  
Build Your Dreams
- D. Release control

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 202**

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

- A. Non-repudiation
- B. Confidentiality
- C. Authentication
- D. Integrity

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 203**

Which of the following characteristics are described by the DIAP Information Readiness

Assessment function? Each correct answer represents a complete solution. Choose all that apply.

- A. It performs vulnerability/threat analysis assessment.
- B. It identifies and generates IA requirements.
- C. It provides data needed to accurately assess IA readiness.
- D. It provides for entry and storage of individual system data.

Build Your Dreams

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 204**

Joseph works as a Software Developer for Web Tech Inc. He wants to protect the algorithms

and the techniques of programming that he uses in developing an application. Which of the

following laws are used to protect a part of software?

- A. Code Security law
- B. Trademark laws
- C. Copyright laws
- D. Patent laws

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 205**

Which of the following is the best method to stop vulnerability attacks on a Web server?

- A. Using strong passwords
- B. Configuring a firewall
- C. Implementing the latest virus scanner
- D. Installing service packs and updates

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Build Your Dreams

**QUESTION 206**

Which of the following is NOT a valid maturity level of the Software Capability Maturity Model (CMM)?

- A. Managed level
- B. Defined level
- C. Fundamental level
- D. Repeatable level

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 207**

Which of the following BCP teams is the first responder and deals with the immediate effects of the disaster?

- A. Emergency-management team
- B. Damage-assessment team
- C. Off-site storage team
- D. Emergency action team

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 208**

Build Your Dreams

Which of the following security models dictates that subjects can only access objects through applications?

- A. Biba-Clark model
- B. Bell-LaPadula
- C. Clark-Wilson
- D. Biba model

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 209**

Which of the following relies on a physical characteristic of the user to verify his identity?

- A. Social Engineering
- B. Kerberos v5
- C. Biometrics
- D. CHAP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 210**

Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

Build Your Dreams

- A. Data downloading from the Internet
- B. File and object access
- C. Network logons and logoffs
- D. Printer access

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 211**

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

- A. Operational audit
- B. Dependent audit
- C. Non-operational audit
- D. Independent audit

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 212**

Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems?

- A. Gramm-Leach-Bliley Act  
Build Your Dreams
- B. Computer Fraud and Abuse Act
- C. Computer Security Act
- D. Digital Millennium Copyright Act

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 213**

You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:

Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

Build Your Dreams

- A. \$142,000
- B. \$232,000
- C. \$41,750
- D. \$23,750

**Correct Answer:** D



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 214**

Which of the following statements about system hardening are true? Each correct answer represents a complete solution. Choose two.

- A. It can be achieved by installing service packs and security updates on a regular basis.
- B. It is used for securing the computer hardware.
- C. It can be achieved by locking the computer room.
- D. It is used for securing an operating system.

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

corrected.

**QUESTION 215**

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A. Editor  
Build Your Dreams
- B. Custodian
- C. Owner
- D. Security auditor
- E. User

**Correct Answer: BCDE**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 216**

Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

- A. Monitor and Control Risks
- B. Identify Risks
- C. Perform Qualitative Risk Analysis
- D. Perform Quantitative Risk Analysis

**Correct Answer:** A

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

#### **QUESTION 217**

Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the Build Your Dreams project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

- A. Project contractual relationship with the vendor
- B. Project management plan
- C. Project communications plan
- D. Project scope statement

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 218**

You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

- A. Risk management plan
- B. Lessons learned documentation
- C. Risk register
- D. Stakeholder management strategy

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<http://www.gratisexam.com/>

<http://www.gratisexam.com/>