**Security Policies**

|  |  |  |
| --- | --- | --- |
| **1.** | Which of the following is not a purpose of a security policy?   1. Define a baseline. 2. Define how to handle security incidents. 3. Define what is and is not allowed. 4. Define the organizational chart. | [*     D. The security policy doesn't define the organizational chart-this is typically defined in a business policy or plan.  *    Answers A , B , and C are defined in a security policy and therefore are incorrect.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N27) |
| **2.** | Which of the following security policy components defines what is and is not allowed regarding an organization's assets?   1. Statement of authority 2. Acceptable use 3. Identification 4. Incident handling | [*     B. Acceptable use defines what is and is not allowed regarding an organization's assets.  *     A defines who is writing the policy and what areas and topics it covers (its scope). C defines what is used to verify a user's identity and restrict access to only authorized resources. D defines the steps taken during and after an incident occurs, to ensure that cool heads prevail during the time of a crisis.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N83) |

**Answers**

|  |  |
| --- | --- |
| **1.** | *  **D.** The security policy doesn't define the organizational chart—this is typically defined in a business policy or plan. *  Answers **A**, **B**, and **C** are defined in a security policy and therefore are incorrect. |
| **2.** | *  **B.** Acceptable use defines what is and is not allowed regarding an organization's assets. *  **A** defines who is writing the policy and what areas and topics it covers (its scope). **C** defines what is used to verify a user's identity and restrict access to only authorized resources. **D** defines the steps taken during and after an incident occurs, to ensure that cool heads prevail during the time of a crisis. |

**Operations Security**

|  |  |  |
| --- | --- | --- |
| **3.** | Which SDLC phase categorizes how a security breach would impact various company assets, resulting in a preliminary risk assessment?   1. Initiation 2. Acquisition 3. Implementation 4. Disposition | [*     A. The initiation phase categorizes how a security breach would impact various company assets, resulting in a preliminary risk assessment.  *     B provides a formal risk assessment of the information found in the initiation phase; in this phase, an analysis of the current security environment, policies, and functional requirements is performed, all the security controls are completely documented, and a pretest of the solution is put in place and tested. With C , the solution is verified and validated by management, the security solution is deployed, and the deployment process is certified. With D , information is retained to meet any legal or government requirements, any unnecessary data is sanitized, and hardware and/or software are disposed of in accordance with the security policy guidelines.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N149) |
| **4.** | Which risk analytical approach uses mathematical models to determine risk, where a dollar loss is associated with various risk and securitythreats?   1. Quantitative 2. Qualitative 3. Quasimodic 4. Avoidance | [*     A. Quantitative analysis uses mathematical models to determine risk, where a dollar loss is associated with various risk and security threats.  *     B lists the components, from a larger perspective, that would be affected by a threat and ranks them based on the likelihood that they would occur, where scenario models are used. C is a nonexistent word. D eliminates risk.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N205) |
| **5.** | Network security testing occurs during which two phases of SDLC?   1. Implementation and disposition 2. Initiation and acquisition 3. Operations and maintenance 4. Implementation and operation | [*     D. Network security testing occurs during the implementation and operation phase of SDLC.  *     B , C , and D are incorrect because they have the incorrect phase combinations.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N266) |
| **6.** | Which of the following is not a technique used during network and vulnerability scanning?   1. Using antivirus tools 2. Using scanning tools like Nessus 3. Performing penetration testing 4. Implementing firewall controls | [*     D. Network and vulnerability is performed to test firewall control network implementation.  *     A , B , and C are used for network and vulnerability scanning and thus are incorrect answers.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N323) |

**Answers**

|  |  |
| --- | --- |
| **3.** | *  **A.** The initiation phase categorizes how a security breach would impact various company assets, resulting in a preliminary risk assessment. *  **B** provides a formal risk assessment of the information found in the initiation phase; in this phase, an analysis of the current security environment, policies, and functional requirements is performed, all the security controls are completely documented, and a pretest of the solution is put in place and tested. With **C**, the solution is verified and validated by management, the security solution is deployed, and the deployment process is certified. With **D**, information is retained to meet any legal or government requirements, any unnecessary data is sanitized, and hardware and/or software are disposed of in accordance with thesecurity policy guidelines. |
| **4.** | *  **A.** Quantitative analysis uses mathematical models to determine risk, where a dollar loss is associated with various risk and security threats. *  **B** lists the components, from a larger perspective, that would be affected by a threat and ranks them based on the likelihood that they would occur, where scenario models are used. **C** is a nonexistent word. **D** eliminates risk. |
| **5.** | *  **D.** Network security testing occurs during the implementation and operation phase of SDLC. *  **B**, **C**, and **D** are incorrect because they have the incorrect phase combinations. |
| **6.** | *  **D.** Network and vulnerability is performed to test firewall control network implementation. *  **A**, **B**, and **C** are used for network and vulnerability scanning and thus are incorrect answers. |

**Secure Network Design**

|  |  |  |
| --- | --- | --- |
| **7.** | Which of the following is the most important factor in a security design?   1. Risk analysis 2. Security policy 3. Business needs 4. Industry best practices | [*     C. Business needs are the most important factor in a security design.  *    Since business needs are the most important, answers A , B , and D are incorrect.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N389) |
| **8.** | What is the most secure method of configuration management?   1. OOB 2. CLI 3. SSL 4. Telnet | [*     A. The most secure method of configuration management is out-of-band (OOB).  *     B , C , and D are incorrect because they could be in-band or OOB.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N445) |
| **9.** | Which of the following is not a key principle for a self-defending network?   1. Integrated security 2. Collaboration 3. Adaptation 4. Firewall controls | [*     D. Firewall controls are one component of integrated security.  *     A , B , and C are incorrect because they are the three principles of a self-defending network.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N502) |
| **10.** | Which of the following is not an active threat defense capability of Cisco's ASA security appliances?   1. Security policy auditing 2. Application inspection and control 3. VPNs 4. Cisco Secure Desktop | [*     A. Cisco's Security Auditor performs security policy auditing.  *    Answers B , C , and D are active threat defense capabilities of Cisco's ASA security appliances, and thus are incorrect answers.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=262172408&rowid=269&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N559) |

**Answers**

|  |  |
| --- | --- |
| **7.** | *  **C.** Business needs are the most important factor in a security design. *  Since business needs are the most important, answers **A**, **B**, and **D** are incorrect. |
| **8.** | *  **A.** The most secure method of configuration management is out-of-band (OOB). *  **B**, **C**, and **D** are incorrect because they could be in-band or OOB. |
| **9.** | *  **D.** Firewall controls are one component of integrated security. *  **A**, **B**, and **C** are incorrect because they are the three principles of a self-defending network. |
| **10.** | *  **A.** Cisco's Security Auditor performs security policy auditing. *  Answers **B**, **C**, and **D** are active threat defense capabilities of Cisco's ASA security appliances, and thus are incorrect answers. |