CISMP Practice Questions ONE

1. When choosing a security critical product to protect sensitive information it BEST to choose ONE which is:
    a. fully guaranteed
    b. evaluated against the common criteria
    c. highly rated by trade journals
    d. certified against iso/iec 27000 series standard

2. If an email message is NOT from the person it claims to be from, this is defined in security terms as:
    a. falsifying
    b. repudiating
    c. masquerading
    d. authenticating

3. A hash is:
    a. something calculated from a set of numbers or bit strings
    b. an encryption technique
    c. a hierarchical approach to managing systems and software
    d. a type of malicious software

4. Why is it important that security incidents are reported promptly?
    a. to ensure rectification and to limit damage or loss
    b. in order to ensure that all people causing incidents are caught
    c. to identify weaknesses in security awareness and training
    d. because the organisations policy says so

5. Bob needs to send a confidential email to alice with confidence it will arrive unaltered. Alice needs to be sure the email is from bob. Bob would use:
    a. his private key only
    b. alices public key and his own private key
    c. alice’s private key only
    d. alice’s private and public key

6. Trojan horse is another name for:
    a. code which accidently causes damage when executed
    b. a boot sector related virus
    c. code maliciously introduced into executable code
    d. code which is triggered by a certain event at a certain time

7. Which of the following is the prime aspect of the business continuity planning process?
    a. testing plans
    b. locating alternative premises
    c. documentation of agreed procedures
    d. identification and prioritization of critical business processes

8. It is vital to gain visible support for the implementation of appropriate information security standards from whom?
   a. the accreditor
   b. senior management
   c. shop floor staff
   d. the customers

9. When would there be a requirement for law enforcement agencies to be informed of a security incident?
   a. when local legislation requires
   b. only with the approval of senior management
   c. at the discretion of the security manager
   d. only when child pornography is involved

10. If a full time employee develops something during company working hours which is relevant to the employer but is not directly related to the employee's job, who owns the intellectual property rights?
    a. neither
    b. the employee
    c. they both have equal shares
    d. the employer

11. Which of the following will be MOST LIKELY to cause a threat to be raised in importance?
    a. size of security department budget
    b. availability of controls to reduce the risk
    c. cost of implementing controls
    d. business impact analysis

12. In order to allow a user to access a computer, the computer's operating system must:
    a. terminate the users session if unacceptable behavior is encountered
    b. request just a user ID/password combination to log in a user
    c. require the user to confirm that they are authorized to access the computer in addition to a valid user id/password logon
    d. alert the system administrator if unacceptable behavior is encountered

13. System security test and evaluation plans SHOULD be specified by:
    a. the systems development test team
    b. the security accreditation authority
    c. the operational authority
    d. information security, the system developer, and relevant operational staff

14. Why SHOULD information be given a classification?
    1. so that people understand the level of confidentiality
    2. so that people understand how to use it
    3. so that people understand how to dispose of it
    4. so that people understand how much it is worth

    a. 1 and 2 only
    b. 1,2 and 3 only
    c. 1,2,3 and 4
    d. 3 and 4 only

15. Phishing attacks are aimed at collecting personal data by using:
    a. phone hacking
    b. emails
    c. hacking tools
    d. brute force attacks

16. Privileged access to a system should be available to:
    a. an authorized person on a needs basis
    b. all system managers and engineers
    c. security auditor
    d. the system supplier and their engineers

17. An organisation’s network is connected to the Internet. The MOST LIKELY threat is from:
    a. Incoming viruses and Trojan Horses
    b. Hackers attempting to bypass the firewall
    c. The organisations staff
    d. Organised crime

18. Malicious code is a type of:
    a. Control
    b. Risk
    c. Vulnerability
    d. Threat

19. System contingency situations…
    a. can be eliminated by thorough testing
    b. will not occur in a well managed organization
    c. can always be covered by insurance
    d. should always be planned for

20. What status SHOULD a security policy have within an organization?
    a. Mandatory
    b. Advisory
    c. Discretionary
    d. Implement where possible