CISMP Practice Questions Four

1. What is the method of identifying unprotected modems connected to your phone system known as?
   a. war walking
   b. war driving
   c. war chalking
   d. war dialling

2. Who should be responsible for classifying an item of information?
   a. the Chief Information Officer
   b. The IT manager
   c. The user of the data
   d. The originator or nominated owner of the data

3. Which voice transmission technique is easily monitored?
   a. PSTN
   b. Mobile/GSM
   c. VoIP
   d. Tetra Radio system

4. An information security policy:
   a. is a public media statement on security in the organization
   b. defines procedures to manage information breaches
   c. sets the basic policy for the protection of information
   d. gives the rules for it department staff

5. In deciding what security measures to implement, an organization should :
   a. implement only as much security as appropriate
   b. adopt a set of standard baseline measures
   c. adopt the same measures as other similar organisations
   d. implement as much security as you can afford

6. The term used when securing an operating system by closing down vulnerabilities and security problems is :
   a. risk management
   b. hardening
   c. bug fixing
   d. change management

7. What do message digests check?
   a. availability
   b. confidentiality
   c. integrity
   d. authentication

8. When outsourcing an information technology contract, whose security policies must be used as part of the contractual conditions?
   a. a “best mix” of the two sets of policies
   b. the organization taking on the work
   c. the organisation outsourcing the work
   d. neither such policies can be used in the contract

9. Formal certification of the security functionality of an IT software product is obtained by:
   a. the owner of the intellectual property rights of the software
   b. the users of the software
   c. the licensees of the software
   d. the owner of the hardware on which the software will be used

10. Assigning security responsibilities to a director of an organization is desirable because?
   a. company legislation requires this
   b. security is too important to be the responsibility only of more junior staff
   c. it s important to know who to blame for the losses
   d. there can be no doubts who is responsible and accountable

11. What is the PRINCIPAL purpose of physical and environmental security?
   a. to prevent theft of equipment and maintain the air conditioning
   b. to keep the IT services running at all times
   c. to prevent unauthorised interference with, access to and damage to IT assets and services
   d. to make it possible for authorized people to access IT assets and services

12. What practice serves to hide secret messages in other messages or images?
   a. steganography
   b. concealment ciphers
   c. hiding ciphers
   d. one time pad

13. Viruses are frequently being transmitted between word processing documents and spreadsheets. These viruses are known as:
   a. macro viruses
   b. parasitic viruses
   c. boot sector viruses
   d. heuristic viruses

14. When it comes to contingency planning, risk assessment is…
   a. something to apply to the plan itself
   b. irrelevant seeing as it is only concerned with security
   c. an essential first step
   d. something to build into the plan

15. How best should security be organized?
    a. as directed by the security manager
    b. as agreed by the department managers
    c. via a formal security organisation
    d. as advised by the auditors

16. A guide developed by an auditor prior to an audit is called a:
    a. Audit report
    b. Procedure
    c. Checklist
    d. Policy document

17. When investigating an incident involving the use of a computer, the MOST appropriate action is to:
    a. allow the user to continue working until a computer forensic expert can examine it
    b. shut down the computer using the normal procedures
    c. make a backup copy of the hard disk and shut down normally
    d. isolate the machine and maintains its power until a computer forensic expert can examine it in situ

18. What is the benefit of token authentication mechanisms utilsing a one time password scheme?
    a. it automates the authentication process
    b. it means a user never has to remember their password
    c. it means the user never has to log on
    d. it prevents the reuse of captured passwords

19. Production software is software which:
    a. is in development
    b. is part of the operating system
    c. is only for use by system programmers
    d. is used to support computer operations

20. Which of the following awareness strategies will encourage a security positive culture?
    1. explaining risks to users so that they understand why they need to protect information
    2. explain to users what action they need to take to protect information
    3. explaining to users what action should be taken if a data breach occurs
    4. explaining to users that the managers know when a data breach occurs
        a. 3 and 4 only
        b. 1 and 2 only
        c. 1 and 4 only
        d. 1,2, and 3 only