CISMP Practice Questions TWO

1. IP spoofing is..
   a. an avialability issue
   b. where an IP address is impersonated
   c. a confidentiality issue
   d. where a node is tampered with

2. A risk assessment finds that the key risks relate to confidential records. The BEST policy for managing security in this case is:
   a. encrypt all confidential records
   b. fully implement all the controls in ISO/IEC27001 and minimize all risks
   c. make a business decision based upon the minimum investment that can be justified
   d. decide what residual risk is acceptable and implement controls to achieve that level

3. The likelihood of fraud can be reduced in an organization by:
   a. imposing serious penalties on those suspected of fraud
   b. requiring all junior staff to sign the official secrets act
   c. the implementation of information security standards
   d. telling staff they are being watched all the time by the management

4. The acronym RAID refers to which of the following:
   a. Redundant Array of Independent Disks
   b. Redundant Array of Indifferent Disks
   c. Resilient Array of Independent Disks
   d. Resilient Array of Information Disks

5. How SHOULD information assets be accounted for?
   a. every user should be responsible for the information resources that they use
   b. the IT manager should be responsible for all information assets
   c. all major information assets should have a nominated owner
   d. their value should be written off the books on acquisition

6. How SHOULD information stored in a cloud hosted environment be deleted when no longer required?
   a. the supplier should destroy the hard drives
   b. the supplier should erase the hard drive contents
   c. the method should be defined in the service agreement
   d. the customer should erase the hard drive contents

7. In addition to securing computer systems and data, an organization should have security controls for:
   a. documents, plans, photographs and anything containing intellectual property
   b. documents, plans and photographs only
   c. any document containing photos and information only
   d. documents only

8. Credit cards use Chip and PIN technology to control:
   a. misposting of credit card transactions
   b. "Card not Present" fraud
   c. Overspending
   d. Credit card fraud

9. Which of the following strategies will help protect information held within the cloud?
   1. classifying data and using the classification to define appropriate controls
   2. anonymising data when testing
   3. encryption of sensitive data
   4. regular destruction of out of date production data
      a. 1 and 2 only
      b. 1,2, and 3 only
      c. 1 and 4 only
      d. 3 and 4 only

10. The theft, disruption and abuse of telephony systems is known as:
    a. hacking
    b. streaking
    c. phreaking
    d. wiretapping

11. Confidentiality, integrity and availability aspects of an information security system are:
    a. some of the management objectives of security
    b. just the main security aspects that need addressing
    c. the key aspects into which all security measures conventionally fall
    d. the security measures required by government

12. What is a demilitarised zone (DMZ)?
    a. an area in a network safe from denial of service attacks
    b. an area used by anti-virus software to quarantine suspected malicious code
    c. an area in a network that allows limited and controlled access from the Internet
    d. an area in a network behind a firewall which is safe against all external attacks

13. How could you protect your investment in expensive software products from the possibility of the supplier going out of business?
    a. by only using software from well known suppliers
    b. keep the media masters in the safe
    c. put the source code and supporting documentation into escrow
    d. include requirements in a service level agreement

14. It is important for a business to have a documented information retention policy to:
    a. ensure that filing cabinets and disks do not get too full
    b. ensure that records are kept for an appropriate amount of time and no longer
    c. save paper by not printing out all data stored
    d. ensure that records are immediately available at all times regardless of the format

15. Which is NOT an example of third party access?
    a. a member of staff dialing in to the company from home
    b. a member of staff searching online on external sites
    c. a member of the public accessing a company's website
    d. a member of the public obtaining money from an ATM machine

16. Security losses sustained on a geographically widespread scale:
    a. are likely to result if poor security is a feature of the wide area network
    b. are inevitable in any large corporate organization
    c. can be avoided with a firewall
    d. should be reported to the treasury department of government

17. The areas that are at highest risk in terms of maintaining the viability of the business…
    a. are the only areas where information security is important
    b. are best assessed only by senior management
    c. are always going to based around IT systems
    d. can be determined by the effective implementation of a recognized security standard

18. What is a Botnet?
    a. a network of computers designed to utilise spare processing capacity
    b. a virus that grows and has the ability to bring down a network\
    c. a self replicating virus
    d. a group of compromised machines capable of being controlled by someone other than their owner

19. How best should staff be informed of their security responsibilities?
    a. circulate regular updates to all staff about recent security incidents and how they could be avoided
    b. publish the security policy and guidance documents on the intranet and corporate notice boards
    c. include security responsibilities in all job descriptions and conditions of employment
    d. provide regular and informal training sessions to staff about current threats and risks

20. The characteristic that defines whether a message has been altered is its:
    a. integrity
    b. authenticity
    c. confidentiality
    d. non-repudiation