True-or-False questions for Module 2: IT and Cyber

1. T/F Information security is about protecting information (data) and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
2. T/F Information security is about protecting information (data) and information systems from unauthorized access, use, disclosure, and less about disruption, modification, or destruction.
3. T/F Information Security management is a process of defining the security controls in order to protect the information assets.
4. T/F Information Security management is a process of defining the security controls in order to protect the information assets.
5. T/F The C.I.A. triangle consists of confidentiality, integrity, and availability.
6. T/F The C.I.A. triangle consists of computers, intrusion, and attacks.
7. T/F Policy, awareness, training, education, technology are necessary tools for information security.
8. T/F The most important tools for information security are technology and training and to a much lesser extent policy, awareness, and education.
9. T/F Software, hardware, or procedural weakness are among the things that can facilitate unauthorized access to a computer by attackers.
10. T/F Vulnerability characterizes the absence or the weakness of a safeguard that could be exploited.
11. T/F A threat is a potential danger to information or systems.
12. T/F A threat is a possibility that someone identifies and exploits the vulnerability.
13. T/F The entity that takes advantage of vulnerability is referred to as a threat agent.
14. T/F The entity that takes advantage of vulnerability is referred to as a vulnerability attacker.
15. T/F An example of a threat agent would be an intruder accessing the network through a port on the firewall.
16. T/F Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact.
17. T/F Threat and risk refer to the same phenomenon.
18. T/F Reducing vulnerability and/or threat reduces the risk.
19. T/F Reducing vulnerability and/or threat does not necessarily reduce the risk.
20. T/F Vulnerability exposes an organization to possible damages.
21. T/F Risk means that an organization will suffer damages that will surely occur.
22. T/F Threat means that an organization will suffer damages that will surely occur.
23. T/F Countermeasure means the same as safeguard in terms of cybersecurity.
24. T/F Safeguard means an application or a software configuration or hardware or a procedure that mitigates the risk while countermeasure means minimizing the consequences after an attack has already occurred.
25. T/F An example of vulnerability would be if a company has antivirus software but does not keep the virus signatures up-to-date.
26. T/F The likelihood of a virus showing up in the environment and causing damage is the risk.
27. T/F The likelihood of a virus showing up in the environment and causing damage is the threat.

28. T/F Installing an antivirus software on all computers is a sufficient protection against threats.
29. T/F Updating the signatures and installing an antivirus software on all computers are an efficient measure against attacks and exploiting vulnerabilities.
30. T/F The best approach to information security is the top-down approach.
31. T/F The best approach to information security is the bottom-up approach.
32. T/F An example of top-down information security management is a lower-end team offering a security control or a program without proper management support and direction.
33. T/F Two of the biggest strengths of the bottom-up information security approach are participant support and organizational staying power.
34. T/F Two of the biggest weaknesses of the bottom-up information security approach are participant support and organizational staying power.
35. T/F Two of the biggest weaknesses of the top-down information security approach are participant support and organizational staying power.
36. T/F Three types of security control are administrative controls, technical or logical controls and physical controls.
37. T/F Three types of security control are administrative controls, technical or logical controls and management controls.
38. T/F Three types of security control are bureaucratic controls, logistic controls and physical controls.
39. T/F Administrative controls, among other things, include screening of personnel and implementing change control procedures.
40. T/F Administrative controls, among other things, include password and resource management and identification and authentication methods.
41. T/F Technical or Logical Controls, among other things, include configuration of the infrastructure and security devices.
42. T/F Technical or Logical Controls, among other things, include developing and publishing of policies, standards, procedures, and guidelines, and implementing change control procedures.
43. T/F Physical controls, among other things, include protecting the perimeter of the facility and controlling individual access into the facility and different departments
44. T/F Physical controls, among other things, include implementing and maintaining access control mechanisms and identification and authentication methods.
45. T/F The following three groups have certain roles and responsibilities for information security: senior management, functional management, and operational managers.
46. T/F Senior management, functional management, and operational managers have roles and responsibilities for information security but not operational staff and lower level managers.
47. T/F An information security project team would include information security officer, system administrators, security administrators but not the end users.
48. T/F An information security project team would include information security officer, system administrators, security administrators but not the data custodian.
49. T/F Information security cannot be achieved through technological tools alone.
50. T/F Technological tools on their own are enough for achieving information security.
51. T/F A system is only as secure as the weakest link.
52. T/F A system is only as secure as its least vulnerable link.