Questions

1. [Q-001] What is the goal of cybersecurity?
   a. The achievement of the security properties
   b. The maintenance of the security properties
   c. All of the above
   d. None of the above

2. [Q-002] What is the definition of accountability?
   a. The property of a system or a system resource being accessible or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system
   b. The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner
   c. The property of a system or system resource ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions
   d. None of the above

3. [Q-003] What is the fundamental concept of the risk assessment?
   a. Identify major hazards in a structured way.
   b. Identify major dangers in a structured way and increase awareness in cybersecurity
   c. Identify the best cybersecurity standard that secures corporate assets
   d. Use analytic and structured processes to capture information and evidence relating the potential for desirable and undesirable events

4. [Q-004] Your company has decided to implement the NIST CSF, who do you call to perform an audit?
   a. The CSO
   b. The security manager
   c. None of the above
   d. All of the above

5. [Q-005] What standard defines the system integrator as a role in the cybersecurity assessment process?
   a. SOGP
   b. IEC 62443

c. ISO 27001
d. None of the above

6. [Q-006] What is the standard that defines the concept of defense in depth?
   a. ISO 27001
   b. SOGP
   c. IEC 62443

7. [Q-007] What are the zones defined by ISO 27001?
   a. a layered security approach
   b. a logical groupings of assets
   c. All of the above
   d. None of the above

8. [Q-008] What are the security maturity levels defined by IEC 62443?
   a. These levels define the benchmarks that are requirements defined by the standards IEC 62443 2-4 and IEC 62443 4-1
   b. These levels measure asset security according to that are the requirements defined by IEC 62443 2-4 and IEC 62443 4-1 standards

9. [Q-009] What are the phases of pre-attack according to the MITRE Att&ck framework?
   a. Weaponize and Deliver
   b. Recon and Deliver
   c. Recon and Exploit
   d. Recon and Weaponize

10. [Q-010] What does the contextualization phase of the Italian cybersecurity framework involve?
    a. The identification of the cybersecurity posture of the organization
    b. The usage of tools to define target profiles on which the assessment is carried out
    c. The evaluation of possible security scopes in order to calculate security metrics

11. [Q-011] The organizational structure for dealing with cybersecurity is a cycle. Within this cycle what task is reserved for the company's Executives??
    a. Assess, communicate and control the security governance
    b. Evaluate, direct and monitor the security governance
    c. Lead the security management function inside the company
    d. Direct, evaluate, monitor and communicate the security governance
    e. All of the above

12. [Q012] What are the elements that define the impact of a threat?
    a. Asset and threat
    b. Threat and vulnerability
    c. Likelihood and threat
    d. All of the above

In the risk determination process the likelihood of an event is given by...

a. The asset and the exposure
b. The vulnerability and the threat frequency
c. The threat capability and the threat frequency
d. None of the above

14. [Q-014] Which is the principle of personnel security that reveals if an employee is involved in malicious activities?
    a. Dual operator policy
    b. Mandatory vacations
    c. Separation of duties
    d. None of the above

15. [Q-015] By the term authorization what kind of function are we identifying?
    a. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
    b. The granting of access or other rights to a user, program, or process to access system resources
    c. None of the above
    d. All of the above

16. [Q-016] If I am implementing DHCP snooping what device am I working on?
    a. Firewall
    b. Switch
    c. Border router
    d. None of the above

17. [Q-017] Is the ISO / IEC 27001: 2013 standard, which defines the requirements for the ISMS, certifiable?
    a. Yes.
    b. No.
    c. It depends on the time of year in which the application to the certification body is made.

18. [Q-018] What is documented information within a management system?
    a. It is information about the leadership of the Organization
    b. When ISO standard states that information must be available as a set of documented information or stored as documented information (and similar), the management system must guarantee written evidence, (e.g in its processes /policies) of such information. This is what documented information means within a management system
    c. It is information reguarding how the Organization relates to others, within the same context

19. [Q-019] What are countermeasures for an ISMS?
    a. It is possible to consider 'countermeasures' those actions that can document information about the scope of the management system
    b. They are measures that can mitigate the information security risk
    c. They are measures to extend the scope or the reach of the ISMS

20. [Q-020] When delivering 'software as a service', what aspects is the cloud service provider responsible for?
    a. Everything but the data
    b. Infrastructure, but not platform and the parts that are above the operating system
    c. Only for network, server maintenance and virtualization

21. [Q-021] What, among the following, does not constitute a common Information security risk in cloud computing?
    a. Multi-tenancy: creating multiple virtual environments logically distinct present on the same physical component, effectively allowing multiple customers (tenants) to work independently, increases the risk of attacks that can compromise this separation and therefore the confidentiality of the data
    b. Not being able to identify the people working behind the delivered cloud service
    c. The increasingly international location of computational and storage systems that makes the localization of processing and storage of data often unidentifiable

22. [Q-022] What is the main purpose of Reg. (UE) 2016/679 (also known as 'GDPR')?
    a. Giving the personal data controller a way to contact data subjects
    b. Informing the data subjects about all the personal data processors involved
    c. Protecting natural persons when their personal data is processed

23. [Q-023] Who is the personal data (PII) controller?
    a. Data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
    b. The data controller is thw natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
    c. The data controller is the natural person whose PII are referred to

24. [Q-024] NIST Framework 'functions' are:
    a. Category, subcategory and informative references
    b. Identify, protect, detect, respond and recover
    c. Risk assessment and threat response

25. [Q-024] How do common criteria arrive at an Evaluation Assurance Level (EAL)?
    a. By assessing the level of innovation brought by the technology to be evaluated
    b. By grouping of security functional requirements divided in classes, allowing specific classes of requirements to be evaluated in a standard way
    c. Through assessment of the risk deriving by external threats

26. [Q-025] Why digital skills frameworks can improve information security in an Organization?
    a. Because the more the skills can be typified and composited, the more it is possible to search for specific skills in the professional figures that one wants to hire for certain jobs, and the workers can test their skills in the same way against the typed criteria
    b. Because digital skill frameworks describe how PII can be processed, helping reducing the risk of compliance to EU privacy law
    c. Because digital skill frameworks can provide for countermeasures to help reduce IT risk

27. [Q-026] For the e-CF, 'attitude' is...
    a. the 'cognitive and relational capacity' (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism...). Attitudes can be defined as a 'glue' which keeps skills and knowledge together.
    b. A way of defining the behaviour of IT systems
    c. The combination of skills and knowledge

28. [Q-027] In the NICE Framework, task statements describe the work, while Knowledge and Skill statements describe the learner
    a. False. Work role describe the work

b. Partially true: the learner is also described by the job position
c. True

29. [Q-028] Cyber Career Pathways Tool (from cisa.gov) is...
    a. ... a tool that offers an interactive way for working professionals (cyber and non-cyber), employers, students, and recent grads to explore and build their own career roadmap across the 52 different NICE Framework work roles
    b. ...a reference framework of ICT knowledge that is used to assess knowledge about electronic communication systems
    c. ...a reference framework of ICT skills that can be used and understood by ICT user and supply companies, ICT practitioners, managers and Human Resources(HR) departments, the public sector, educational and social partners across Europe

30. [Q-029] For the purposes of the ISO/IEC 17024:2012, what is a certification process?
    a. It is a process of assessing information security risk against specific criteria
    b. It is a process of assessing if competences for specific ICT job positions are met
    c. It is a set of activities by which a certification body determines that a person fulfils certification requirements, including application, assessment, decision on certification, recertification and use of certificates and logos/marks

31. [Q-030] What is DoDD 8140?
    a. DoD Directive 8140 establishes a definition for the cyber workforce and outlines component roles and responsibilities for the management of the Department of Defence cyber workforce
    b. DoD Directive 8140 is a method for addressing countermeasures for IT systems involved in the military workplace
    c. DoD Directive 8140 defines the requisites for certifying people against ISO/IEC 27001:2013

32. [Q-031] An accreditation body is...
    a. ...the body that performs conformity assessment services
    b. ...an authoritative body that performs accreditation. The authority of an accreditation body is generally derived from government.
    c. ...an authority derived from the DoD

33. [Q-032] Use case for ISO/IEC 27001 ISMS audit. The auditor notes that the people in the Beta LLP company are in a hurry, they exchange information in the corridors, they switch roles to help each other. The auditor then decides to interview staff about their role awareness and information security policies. 13 out of 18 people did not know about the information security policy, or did not know where to find it.
    a. This scenario is average in many Organizations, from different business fields. No action is then required from Beta LLP
    b. This situation is very serious because people must have a defined role and responsibility to be aware of. Also, people are not aware of the security policy
    c. This situation might jeopardize information security because not enough budget is allocated to reduce the risk of incidents