Title: "Security and risk: management and certifications" 2021-2022 - SCQ0089517

Lecturers: *Prof. Simone Soderi, Prof. Antonio Belli*

Examination: Written examination: 16th June, 2022 at 10:30 – 12:30

Assessment: 100% Written examination

Classroom: 2AB/45

==

Student (Surname, Name): ....

Student ID (Matricola): ....

==

Questions

1. **[Q-001] What does the cyber space include?**
   a. Interconnection of IoT devices
   b. Information exchanged between virtual machines
   c. Information, interconnections and artifacts based on computer and communications technology

2. **[Q-002] What is the definition of authenticity?**
   a. The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner
   b. The property of being genuine and being able to verify that users are who they say they are and that each input arriving at the system came from a trusted source
   c. The property that data is not disclosed to system entities unless they have been authorized to know the data

3. **[Q-003] In the risk management process, what are the risk classifications?**
   a. Intolerable, sufficient, catastrophic
   b. High, Medium, very low
   c. Intolerable, tolerable, acceptable
   d. None of the above

4. **[Q-004] What is included by a policy?**
   a. Standard
   b. Guidelines
   c. Control objectives
   d. Procedures
   e. All of the above

5. **[Q-005] What are the main activities of the Standard Of Good Practice (SOGP)?**
   a. Assessment of cybersecurity, management of cybersecurity and risk evaluation
   b. Planning for cybersecurity, managing the cybersecurity function and security assessment
   c. Assessment of cybersecurity, management of cybersecurity

d.

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 conduits?
   a. Conduits are the special type of security zone that groups communications that can be logically organized into zones. It can be a single service or be a multiple data carrier.
   b. Conduits are the special type of security zone that groups communications that can be logically organized into information flows within and also external to a zone. It can be a single service or be a multiple data carrier.
   c. None of the above

8. **[Q-008] What is the principle on which misuse detection is based?**
   a. It uses pattern matching algorithms operating on activities that are different from the normal behaviour
   b. It uses pattern matching algorithms operating on known attacks
   c. It is based on machine-learning techniques that combine known attacks and malicious behaviour.

9. **[Q-009] In the case of zero-day malware, which intrusion detection system is most effective?**
   a. Antivirus
   b. Misuse detection
   c. Anomaly detection

10. **[Q-010] What is the purpose of having a business continuity plan and which is the parameter improved?**
    a. It enhances the disaster response and improves the working hours
    b. It mitigates the effects of disasters and increases the business downtime
    c. It mitigates the effects of disasters and improves the recovery time
    d. All the above

11. **[Q-011] What are the principles for personnel security?**
    a. Least privileges and separate duties
    b. Cybersecurity awareness, separation of duties and dual operator policy
    c. Dual operator policy, separation of duties and limited reliance on key employees
    d. None of the above
    e. All of the above

12. **[Q012] Which is the guideline to follow for equipment disposal?**
    a. IEC 62443-1
    b. NIST Cybersecurity Framework (CSF)
    c. ISO 27001
    d. OWASP
    e. None of the above

13. [Q-013] Which action should be applied to a hard-disk that contains low-level classified data and for which the hard-disk is scheduled to be reused?
   a. Clear
   b. Purge
   c. Destroy
   d. Purge and Clear
   e. None of the above

14. [Q-014] To which authentication means does the password belong?
   a. Possession factor
   b. Knowledge factor
   c. Personal Identification
   d. Logical authentication factor

15. [Q-015] To implement a Layer 3 VPN what is the technology you would choose?
   a. OpenVPN
   b. IPSec IKEv2
   c. None of the above

16. [Q-016] Where can I apply the access control list and what attacks can it mitigate?
   a. Firewall and reconnaissance attacks
   b. Border router IP address spoofing and privilege escalation
   c. Border router IP address spoofing and TCP SYN flooding
   d. None of the above

17. [Q-017] What is an Information security management system?
   a. An ISMS is a tool that companies use to produce evidence of technology usage
   b. An ISMS is a management system designed to protect the information assets of the Organization at the required level of security, through the definition and maintenance of a series of policies, procedures, control / governance tools and best practices
   c. An ISMS is a set of procedures, technologies and instructions

18. [Q-018] What are the phases of the 'Deming' Cycle, applicable to management systems?
   a. Plan, do, check, be aware
   b. Prevent, detect, recover, respond
   c. Plan, do, check, act

19. [Q-019] What is the context for an ISMS?
   a. Context is given by factors that can be internal and external to the Organization, which affect its purposes and may affect the relative ability to achieve the objectives set for the Information Security Management System
   b. Context is a set of circumstances determined by risk analysis
   c. Context is what makes leadership essential

20. [Q-020] What are the main types of cloud services deliverable by a cloud service provider (CSP)?
   a. IaaS (Information as a Service), PaaS(Platform as a Service), DaaS (Delivery as a Service)
   b. IaaS (Infrastructure as a Service), PaaS(Platform as a Service), SaaS (Software as a Service)
   c. CaaS (Configuration as a Service), PaaS(Platform as a Service), MaaS (Management as a Service)

[Q-021] In the shared responsibility model for cloud computing services, the responsibility moves towards the provider...

a. ...The more the technologies are managed by the customer
b. ...The more the components on which the cloud services are based are managed by the provider
c. ...when the cloud services are terminated by the customer before the contract ends

22. [Q-022] How can we define sensitive PII, within the ISO/IEC29100:2011 standard?

a. As data that are processed in a way that makes them more sensitive to the risk of undue disclosure
b. As data that are stored in a manner that exposes them to the risk of alteration and cancellation
c. As a category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal

23. [Q-023] Who is the personal data (PII) processor?

a. Data processor is a natural or legal person, public authority or agency or other body which processes the data on behalf of the controller
b. The data processor is the person who establishes the purposes and methods of the processing
c. The data processor is the legal person who check if information are correct

24. [Q-024] What increases with the Uptime Institute TIER level against which a data center can be certified?

a. The size of the data center
b. Redundancy of components that can ensure power, the ability to be concurrently maintained and being fault tolerant
c. The possibility of providing several different services

25. [Q-025] Does the NIST framework allow for prioritizing the security needs of organizations?

a. Yes, through the adoption of individual organizational Profiles
b. No, NIST Framework is not customizable
c. It just depends on the certification schemes owned by the organization

26. [Q-026] Among other things, what distinguishes the CINI framework from the NIST original version?

a. Nothing. They are identical
b. The CINI framework is only applicable to organizations that process sensitive data
c. Adding a contextualization process and specific controls relating to European privacy law constitute two differences

27. [Q-027] What can Common Criteria be useful for?

a. The Common Criteria enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements
b. The Common Criteria can demonstrate compliance with the personal skills of those who have to evaluate technologies
c. The Common Criteria demonstrate compliance with the security rules of management systems

28. [Q-028] European e-Competence Framework (e-CF) is...

a. ...a reference framework of ICT competences used to determine the skills required for information security only related job positions

b. ...a reference framework of ICT competences that is used to assess knowledge about electronic communication systems

c. ...a reference framework of ICT competences 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

29. [Q-029] What is skill for the e-CF?

a. Skill is everything that relates to the knowledge of a person

b. Skill is defined as "ability to carry out managerial or technical tasks". Managerial and technical skills are the components of competences and specify some core abilities which form a competence

c. Skill equals to "competence"

30. [Q-030] In the NIST - NICE framework, what does describe the work?

a. The task

b. The knowledge

c. The skill

31. [Q-031] Who is affected by DoD Directive 8140?

a. Any full-or part-time military service member in the U.S., contractor, or local nationals with privileged access to a Department of Defense information system performing information assurance (security) functions –regardless of job or occupational series

b. Anyone who has to handle sensitive information concerning people's health within the U.S. Department of Defence

c. Those who need to participate in tenders in the USA

32. [Q-032] A Conformity Assessment Body (CAB) is...

a. ...An authoritative body that performs accreditation of international assessment forums

b. ...The body that performs conformity assessment services and can certify people, products or management systems

c. ...An Organization that facilitates trade and supports regulators by operating a worldwide mutual recognition arrangement among Accreditation Bodies

33. [Q-033] Use case for ISO/IEC 27001 ISMS audit. The Alpha company sets the goal for its ISMS to protect classified information that is very sensitive to be processed. The information security policy does not include any reference to confidential documents and how to protect them.

a. This is a problem as not enough resources have been guaranteed to achieve the stated goal

b. This scenario highlights an unfulfilled requirement of the standard. The objectives of the ISMS must be consistent with the general security policy

c. This does not represent a problem as confidential information is in fact kept as confidential as possible