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

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)

21. **[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

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

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

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)

21. **[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

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

13. **[Q-013] 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

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

ent (Surname, Name): .....

dent ID (Matricola): .....

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

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

1) 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

2)To which authentication means does the password belong?

a. Possession factor
b. Knowledge factor
c. Personal Identification
d. Logical authentication factor

3)To implement a Layer 3 VPN what is the technology you would choose?

a. OpenVPN
b. IPSec IKEv2
c. None of the above

4)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

5)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 èplicies, procedures, control / governance tools and best practices
c. An ISMS is a set of procedures, technologies and instructions

6)What are the phases of the ‘Deming’ Cycle, applicable to management system?

a. Plan, do, check, be aware
b. Prevent, detect, recover, respond
c. Plan, do, check, act

7)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

8)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 (Information 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)

9)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

10)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

11)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

12)NIST Framework 'functions' are:

a. Category, subcategory and informative references
b. Identify, protect, detect, respond and recover
c. Risk assessment and threat response

13)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

14)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

15)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

16)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

17)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

18)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

19)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

20)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

21)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

22)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

23)Which is the principle of personnel security that reveals if an employee is involved in malicious activities?t 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

24)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

25)If I am implementing DHCP snooping what device am I working on?

a. Firewall
b. Switch
c. Border router
d. None of the above

26)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.

27)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

28)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

29)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

30)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

31)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"

32)In the NIST - NICE framework, what does describe the work?
a. The task
b. The knowledge
c. The skill

33)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

34)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

35)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

36)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

37)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 a 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

38)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

39)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

40)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

41)What is the standard that defines the concept of defense in depth?

a. ISO 27001
b. SOGP
c. IEC 62443

42)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

43)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

44)What are the phases of pre-attack according to the METRE Att&ck framework?

a. Weaponize and Deliver
b. Recon and Deliver
c. Recon and Exploit
d. Recon and Weaponize

45)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

46)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

47)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

48)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

49)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

50)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

51)What is included by a policy?

a. Standard
b. Guidelines
c. Control objectives
d. Procedures
e. All of the above

52)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

53)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

54)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

55) 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

56)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

57)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

58)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

59)In the shared responsibility model for cloud computing services, the responsibility moves toward the provider…

a. …The more the technologies are manages by the costumer
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

60)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

61)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.

62)In the case of zero-day malware, which intrusion detection system is most effective?

a. Antivirus
b. Misuse detection
c. Anomaly detection

63)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

64)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

65)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

66)What does ISMS stand for?

a. International System Management Standard
b. Information Security Management System
c. Integrated Security Monitoring System
d. Internet Security Management Service

67)What does a policy comprise?

a. A standard
b. Guidelines
c. Control objectives
d. Procedures
e. All of the options

68)What are the key tasks of the Standard Of Good Practice (SOGP)?

a. Cybersecurity assessment, cybersecurity management, and risk evaluation
b. Cybersecurity planning, cybersecurity function management, and security appraisal
c. Cybersecurity assessment, cybersecurity management

69)Which standard introduces the concept of defense in depth?

a. ISO 27001
b. SOGP
c. IEC 62443

70)How can we describe accountability in the context of a system?

a. It is the property that ensures system or system resources are operational demand by an authorized entity, according to the system's performance
b. It is the property ensuring that data has not been lost, destroyed, o unauthorized or accidental way.
c. It is the property that allows system or system resource actions t an entity, holding that entity responsible for its actions.
d. None of the above.

71)According to the MITRE Att&ck framework, what stage…. phase?

a. The Weaponize and Deliver stages
b. the Reconnaissance and Deliver stages
c. the Reconnaissance and Exploit stages
d. the Reconnaissance and Weaponize stages

In the cycle that represents the organizational structure for cybersecurity, what role is assigned to the company's executives?

a. Assess, communicate, and control security governance
b. Evaluate, direct, and monitor security governance
c. Lead the security management function within the company
d. Direct, evaluate, monitor, and communicate security governance
e. All of the above (?)

73)What function is implied by the term 'authorization'?

a. Checking the identity of a user, process, or device, usually a prerequisite to grant access system resources
b. Permitting a user, program, or process to access system resources
c. None of the above
d. Both a and b

74)What type of authentication does a password fall under?

a. Ownership factor
b. knowledge factor
c. Personal identification
d. Logical authentication factor

75)What determines the level of assurance in the Common Criteria?

a. The analysis and development phases only
b. The extent and formality of documentation only
c. The development methods only
d. Both the documentation and development aspects

76)According to the text, how is a 'skill defined in the context of the European e-CF?

a. The ability to carry out managerial or technical tasks
b. The ability to perform physical tasks efficiently
c. Only to the ability to communicate effectively in a team
d. Specifically to the ability to learn and adapt quickly

77)During the ISO 27001 audit of Gamma Corporation, a company that produces photo and video content upon request and requires certification to safeguard its business, it was discovered that the risk assessment process includes a risk catalogue encompassing numerous potential risk scenarios. Although the overall risk level is low, Inadequate descriptions were found for certain backup-related risks. The candidate is tasked with determining whether this situation poses a problem and, if so, explaining the reasons behind it.

a. Yes, this constitutes a problem. The ISO 27001 standard requires that all risks, including those related to backups, are adequately identified and assessed. Incomplete descriptions of risks related to backups can lead to insufficient mitigation measures and potential data loss or system failures.
b. No, this does not constitute a problem. While it is important to have well-described risks related to backups, the overall risk level being low indicates that the organization has effectively addressed the major risks. The focus should be on high-risk areas, and minor gaps in risk descriptions can be addressed during the next risk assessment cycle.
c. No, this does not constitute a problem. ISO 27001 does not specifically mandate detailed descriptions of risks related to backups. As long as the overall risk level is low, the organization prioritize addressing higher-risk areas, and minor gaps in risk descriptions can be addressed as continuous improvement.
d. No, this does not constitute a problem. The risk assessment process of the Gamma Corporation is already comprehensive, covering numerous risk scenarios. While improvements in risk assessment process for backups would be beneficial, it does not invalidate the overall effectiveness of the (?) process.

78)The levels of the Tier (Uptime Institute) certifications are ...

a. Tier I, 'Recovering Capacity', Tier II 'Identifying Capacity', Tier III 'Protecting Capacity, Tier IV 'Detecting Capacity
b. Tier I, 'Basic Capacity', Tier II 'Redundant Capacity', Tier III 'Concurrently Mantainable', Tier IV 'Fault Tolerant'
c. Level I 'Redundancy', Level II 'Mantaining', Level III 'Recovering

79)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 does not represent a problem as confidential information is in fact kept as confidential as possible
c. This scenario highlights an unfulfilled requirement of the standard. The objectives of the ISMS must be consistent with the general security policy

80)Which guideline is recommended for equipment disposal?

a. IEC 62443-1
b. NIST Cybersecurity Framework (CSF)
c. ISO 27001
d. OWASP
e. None of the above

81)What is the core principle of risk assessment?

a. To methodically identify major threats.
b. To increase cybersecurity awareness by identifying major risks in a structured way.
c. To select the best cybersecurity standard for securing corporate assets.
d. To employ analytical and structured methods to gather information and evidence related to potential positive and negative outcomes.

82)On what principle does misuse detection operate?

a. It employs pattern matching algorithms that operate on activities diverging from the normal behaviour
b. It utilizes pattern matching algorithms that work on identified attacks
c. It is based on machine-learning techniques that combine known attacks and malicious behaviour.

83)What is an important aspect for leadership under ISO/IEC 27001?

a. Determining if leadership is internal or external to the Organization, and then describing the purposes of the organization
b. Determining the results of risk analysis
c. Obtaining the commitment of the Management

84)Cloud computing is...

a. ...Data processing delivered as a service over a network, typically the Internet
b. ...Exclusively delivering platforms as a service
c. ...Exclusively delivering infrastructure as a service

85) In quantitative risk assessment if the cost of security controls is low the total cost of security investment is

a. Low
b. Medium
c. High

86) In qualitative risk determination what is required to determinize the impact?

a. Threat Capability and Vulnerability
b. Threat Frequency and Likelihood of Event
c. Asset and Exposure
d. Asset and Likelihood of Event
e. None of the above

87) Which are the main steps of the incident response life-cycle?

a. Preparation, normalization, analysis and detection
b. Preparation, detection, analysis and post-incident activity
c. None of the above
d. All the above

88)In the STRIDE threat model which phase is relevant to control the integrity?

a. Spoofing identity
b. Tampering with data
c. Repudiation
d. Information Disclosure
e. Denial of Service
f. Elevation of Privilege

89) When I use the MITRE ATT&CK framework, if I want to understand what an opponent gains by performing an action what am I referring to ?

a. Tactic
b. Technique
c. All of the above
d. None of the above

90) ISO/IEC 27001 ..

a. …Guarantees the permanent reduction of the information security risk (NO)
b. Establishes what are the specific configurations of a firewall and an IPS
c. ...Defines a set of rules to run an ISMS