RESILIA™ Foundation

Sample Papers Terms of Use – English

Please note that by downloading and/or using this document, you have agreed to comply with the terms of use outlined below:

1. All sample (electronic or paper based) papers are for personal use only.

2. The sample papers are intended for the following use only:

   - For use as study aid/s for candidates who wish to sit an RESILIA Foundation examination, or

   - for reference purposes.

3. By downloading a complimentary digital copy of any of the RESILIA Foundation sample papers, you agree not to:

   - Reproduce or copy;

   - forward or share;

   - sell the document with/to any third party.

4. If you wish to use the whole or part, of any of this sample paper, for any purpose other than self-study or reference, please contact AXELOS Accreditation Team (examinations@axelos.com).

RESILIA Foundation Examination

Sample Paper 2

Multiple Choice

Exam Duration: 1 hour and 40 minutes

Instructions

1. **All 50 questions should be attempted. Each question is worth one mark.**
2. **All answers are to be marked on the answer sheet provided.**
3. **Use a pencil (NOT ink pen) to mark your answers on the answer sheet provided. There is only one correct answer per question.**
4. **You have 1 hour 40 minutes to complete this paper.**
5. **The exam is closed book i.e. no material other than the *Question Booklet* and the *Answer Booklet* is to be used.**

This is a blank page

1. What is the purpose of a detective control?

   a) It is intended to prevent an incident from occurring
   b) It is intended to identify the occurrence of an incident
   c) It is intended to respond to an incident after it occurs
   d) It is intended to correct the situation after an incident

2. Which is the MAIN result of increased sharing of data?

   a) Integrity of the data may be compromised
   b) New endpoint controls may be needed
   c) New security technologies may be required
   d) New business opportunities may be created

3. Which describes how organizations BEST manage the risk of cyber attacks?

   a) Use their industry's standard approach
   b) Define an approach based on their own risk appetite
   c) Use different approaches for positive and negative risks
   d) Reduce impact by following all industry risk methodologies

4. Which is MOST likely to be a risk?

    a) Sensitive data stored on a PC
    b) Users not trained on security issues
    c) Unencrypted confidential data
    d) Regulator may impose a fine

5. What process identifies new threats and creates an updated risk assessment?

    a) Risk retention and sharing
    b) Risk monitoring and review
    c) Risk analysis and evaluation
    d) Risk treatment and acceptance

6. Which is a risk treatment method?

    a) Risk retention
    b) Risk mitigation
    c) Risk control
    d) Risk tolerance

7. Providing multiple independent controls for cyber resilience is an example of what?

   a) Defence-in-depth
   b) Risk sharing
   c) Continual integration
   d) Risk transfer

8. Which is the BEST use of a management system?

   a) To guide and control organizational work
   b) To ensure security of people and process
   c) To control service and product deliverables
   d) To ensure adherence to best practices

9. What is the BEST description of management activities?

   a) To evaluate, direct and monitor to ensure expectations are met
   b) To plan, build, run and improve efficiency and effectiveness
   c) To document activities, inputs, outputs and interfaces to guide activities
   d) To define responsibilities, activities and authorities to people or teams

10. Which cyber resilience activity should be aligned with IT service strategy?

    a) Understanding the roles and responsibilities for a cyber resilience team
    b) Understanding the business requirements for cyber resilience
    c) Defining a service catalogue for cyber resilience assets
    d) Defining requirements for cyber resilience audits

11. Which is a stakeholder category for a cyber resilience strategy?

    a) Insurance underwriters
    b) Security standards bodies
    c) Target customer markets
    d) Legal and regulatory authorities

12. Which is an external audit activity for cyber resilience?

    a) Defining the audit success criteria
    b) Allocating responsibility for implementing controls
    c) Ensuring the organization is prepared
    d) Providing formal confirmation of conformance

13. Which control ensures that cyber resilience is adequately addressed?

    a) System acquisition and development
    b) Secure use of systems
    c) Control performance evaluation
    d) Cyber resilience governance

14. Which are the BEST sources of documented evidence for cyber resilience compliance?

    a) Service response logs, change logs, and service desk call logs
    b) System logs, device logs and transaction logs
    c) Facility access logs, security logs and customer request logs
    d) Inventory logs, release logs and risk logs

15. Which process would BEST help a business to understand the value of the cyber resilience aspects of a service?

    a) Change evaluation
    b) Design coordination
    c) Financial management
    d) Service level management

16. Which is a purpose of cyber resilience design?

    a) To decide how controls will be funded
    b) To decide how information will be classified
    c) To assess changes to understand their impact
    d) To test controls to ensure they work as expected

17. Which process ensures that security requirements are included in systems that are developed by third parties?

    a) The procurement process
    b) The development process
    c) The demand management process
    d) The service level management process

18. Which control MOST helps to prevent careless or accidental disclosure of information?

    a) Physical security
    b) Operations security
    c) Endpoint security
    d) Human resource security

19. Which suppliers should be included in risk assessment and testing?

    a) All suppliers
    b) New suppliers
    c) Key suppliers
    d) Outsourced IT service suppliers

20. Which control(s) should be used to secure endpoints?

    a) Encrypt storage on the server and its network connection to the endpoint
    b) Encrypt storage on the endpoint and its connection to the organization's network
    c) Encrypt storage on the server and storage on the endpoint
    d) Encrypt confidential data stored on the endpoint

21. What control can protect communication over untrusted networks?

    a) Encrypt communication across untrusted networks
    b) Use network security management on untrusted networks
    c) Never allow data to travel over untrusted networks
    d) Include security requirements in contracts for untrusted networks

22. Which services must have a business continuity plan?

    a) Critical services
    b) Cloud services
    c) Internal IT services
    d) All services

23. What types of controls are developed in availability management?

    a) Preventative controls
    b) Supportive controls
    c) Investigative controls
    d) Recovery controls

24. Why is it important for cyber resilience to identify when business or IT changes are planned?

    a) In order to design a new or updated management system, update the risk register and redefine the roles and accountabilities of staff
    b) In order to review impact on cyber resilience, to update risk assessments and to design, test and implement the required security controls
    c) In order to evaluate the proposed new, or changed, processes for management of cyber resilience and the required controls
    d) In order to improve the handling of transitions to support the need for agility without compromising cyber resilience and minimizing downtime

25. What is the BEST approach to cyber resilience application-security testing?

    a) It should be included throughout the development process
    b) It should be done with user acceptance testing prior to transition
    c) It is best done using case scenarios and user stories
    d) It takes place at the beginning of the Software Development Lifecycle

26. What does a disposal policy need to take into consideration?

    a) How the information has been classified
    b) Who is authorized to access the information
    c) How the information is managed and used
    d) The encryption standard for media disposal

27. Which types of asset do organizations need in order to operate?

    a) Software assets
    b) Technical assets
    c) Service assets
    d) Critical assets

28. Which cyber resilience control visually conveys the importance of an asset and its desired protection?

    a) Classification and handling
    b) Asset and configuration management
    c) Information handling
    d) Document management

29. What must be included in cyber resilience training for all staff?

    a) Data protection, acceptable use policy and change management rules
    b) Secure data handling, data protection and acceptable use policy
    c) Secure operating procedures, data protection and incident process
    d) Secure data handling, secure operating procedures and firewall rules

30. What is best practice for managing business critical documents that contain sensitive information?

    a) They are reviewed regularly and duplicated to prevent loss
    b) They are kept locked in a definitive media library (DLM)
    c) They are password protected with a two level challenge
    d) They are kept up to date and subject to controlled circulation

31. Which process BEST helps to manage organizational change and ensure the success of cyber resilience projects?

    a) Release and deployment management
    b) Transition planning and support
    c) Service validation and testing
    d) Design coordination

32. How does transition planning and support contribute to cyber resilience?

    a) By providing knowledge transfer to ensure that users are aware of any responsibilities for new or changed services
    b) By reviewing infrastructure changes for their potential impact on security controls
    c) By ensuring new or changed services are introduced with attention to the risks they pose
    d) By providing guidance on what risk management activities are needed during service transition

33. In the Operations stage, which of the following statements BEST describes the objectives of cyber resilience controls?

    a) To prevent, to detect and to correct
    b) To detect, to register and to classify
    c) To identify, to classify and to correct
    d) To prevent, to audit and to report

34. Which user activities are ESPECIALLY important to monitor?

    a) Logon success and failure
    b) Locked accounts
    c) Source and destination IP-address
    d) Password changes

35. Which control allows support personnel to help users with local issues?

    a) Wireless access
    b) External network connections
    c) Remote maintenance
    d) Cryptography

36. Which threats are BEST managed with physical access control?

    a) Hackers trying to access systems remotely
    b) Suppliers leaking sensitive information
    c) Hackers trying to enter secure buildings
    d) Users leaking sensitive data through e-mail

37. Which is the MOST appropriate mechanism to protect an organization with a mobile workforce from exposing sensitive information?

    a) To use full disk encryption
    b) To implement incident management
    c) To enforce clear desk policy
    d) To deploy perimeter security

38. What must be the INITIAL objective for an incident response team?

    a) To collect data and carry out forensic analysis to pursue the perpetrator(s)
    b) To isolate the incident and prevent further damage being caused
    c) To identify the root cause of the incident to prevent it from happening again
    d) To design security controls to reduce the impact of the incident

39. Which is MOST likely to be a security incident?

    a) An employee leaves confidential paper documents on a bus
    b) A series of outages due to full disks in a storage solution
    c) Lost internet connectivity due to maintenance at a supplier
    d) Upgrading firmware on a router to address a code vulnerability

40. Which process can BEST help detect a change of state of an IT device, which could be a potential cyber threat?

    a) Incident management
    b) Event management
    c) Problem management
    d) Access management

41. How may the service desk contribute to cyber resilience?

    a) By providing packaging for cyber resilience releases
    b) By defining test criteria for cyber resilience releases
    c) By conducting initial assessment of cyber resilience incidents
    d) By ordering change evaluation after cyber resilience incidents

42. Which can be used as a cyber resilience maturity model?

    a) The AXELOS Management of Risk (M_o_R ®) framework
    b) The National Institute of Standards and Technology (NIST) cyber security framework
    c) The Deming plan-do-check-act (PDCA) cycle
    d) The ITIL continual service improvement (CSI) approach

43. What is the MAIN reason for performing audit and review?

    a) Because it is mandated by the executive board
    b) To match the strategy to the cyber resilience controls
    c) To recommend improvements to the risk standard
    d) Because cyber resilience risks are always changing

44. Which is included in an assessment of non-technical controls?

    a) Review of server patch history
    b) Review of firewall design
    c) Review of physical site logs
    d) Review of anti-virus logs

45. What improvement opportunity can be identified by a post-incident review?

    a) The need for a new risk assessment methodology
    b) New training requirements for the response team
    c) Updates to the cyber resilience strategy
    d) Updates to the service catalogue

46. What do senior management consider when approving improvements?

    a) Selecting a reputable supplier for each recommendation
    b) Identifying recommendations that are cheapest to implement
    c) Balancing the costs and benefits of each recommendation
    d) Implementing recommendations to mitigate highest risks

47. How are the findings of a review and audit BEST presented?

    a) In a format that includes a comprehensive report
    b) In a format illustrated with graphs and tables
    c) In a format that the authors are most familiar with
    d) In a format that the audience can understand

48. In the 'present and use the information' step of the seven-step improvement process for cyber resilience, what audience should be considered?

    a) The cyber resilience technical staff and management
    b) The Executive board and IT management
    c) The Chief Financial Officer and junior management
    d) The customer information security representative

49. What action takes place at the ‘How do we keep the momentum going?’ stage of the CSI approach?

    a) Design metrics to measure the progress of the improvement project
    b) Set measurable targets for the cyber resilience improvements
    c) Ensure that the improvements have been embedded into the organization
    d) Hold a launch meeting to communicate the improvement plan and targets

50. Which is an example of a violation of segregation of duties (SoD)?

    a) Employee 1’s role is network administrator; employee 2’s role is security administrator
    b) Employee 1’s role is network administrator; employee 1’s role is also incident manager
    c) Employee 1’s role is access authorization; employee 1’s role is also security management
    d) Employee 1’s role is developer; employee 2’s role is programmer

This is a blank page