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

Rationale

Multiple Choice Questions

June 2015 Release

1. Syllabus Topic: 1.3 b)
   Correct Answer: B
   Assessment Criteria: Identify the terms: preventative detective and corrective controls (1.4.6/1.5.7).

   a) A is the purpose of a preventative control.
   b) “Detective controls are intended to identify the occurrence of an incident that jeopardizes Cyber Resilience, so that the organization can respond appropriately” (1.4.6).
   c) C is a purpose of corrective controls.
   d) D is a purpose of corrective controls.

2. Syllabus Topic: 1.4 c)
   Correct Answer: D
   Assessment Criteria: Identify the purpose of balancing: risks and opportunities (1.5.1).

   a) A is wrong because increased sharing may affect confidentiality of the data but is unlikely to affect its integrity.
   b) B may be true, depending on the circumstances, but it is important for cyber resilience personnel to understand the balance of risks and opportunities, and not to see everything as a negative risk. Increased sharing of data will normally be done to create business opportunities.
   c) C may be true, depending on the circumstances, but it is important for cyber resilience personnel to understand the balance of risks and opportunities, and not to see everything as a negative risk. Increased sharing of data will normally be done to create business opportunities.
   d) “Increased sharing of data can result in new business opportunities and increased efficiency” (1.5.1).

3. Syllabus Topic: 2.1
   Correct Answer: B
   Assessment Criteria: Describe what risk management is (2.0 up to but not including 2.1 onwards).

   a) Each organization is different.
   b) “Each organization will have a different tolerance for risk, and it is the responsibility of the board of directors (or equivalent) to define the risk appetite and the approach to be taken to managing risk” (2.0).
   c) Each organization is different.
   d) Following all industry methodologies may not reduce impact.

4. Syllabus Topic: 2.3
   Correct Answer: D
   Assessment Criteria: Identify the terms: risk, asset, vulnerability, threat (2.2).

   A, B and C are vulnerabilities. A could also be an asset (Table 2.2).

5. Syllabus Topic: 2.4 f)
   Correct Answer: B
   Assessment Criteria: Describe actions to address risks and opportunities: risk monitoring and review (2.3).

   "There must be a process in place to monitor and review risks to ensure that new threats are identified and result in updated risk assessments" (2.3.6).

6. Syllabus Topic: 2.4 e)
   Correct Answer: A
   Objective: Describe actions to address risks and opportunities: risk treatment (2.3).

   Methods of treating risk – avoidance, modification, sharing and retention (Table 2.3).

7. Syllabus Topic: 2.5 g)
   Correct Answer: A
   Assessment Criteria: Identify the term: defence-in-depth (2.3.5).

   Defence-in-depth is using multiple independent security controls to provide redundancy. Other answers are invalid (2.3.5.2).

8. Syllabus Topic: 3.1
   Correct Answer: A
   Assessment Criteria: Identify the purpose and scope of a management system (3.1).

   a) “Every organization has a management system that is used to guide and control the work it carries out” (3.1).
   b) This is not the best use, there are other needs.
   c) This is not the best use, there are other needs.
   d) This is not the best use, there are other needs.

9. Syllabus Topic: 3.4
   Correct Answer: B
   Assessment Criteria: Describe the difference between management, governance (3.1) and compliance (4.1.4.2).

   a) Governance Activities.
   b) Management activities are to plan, build, run and improve the business. “Management allocates resources, makes tactical and operational decisions and oversees activities to ensure they are carried out efficiently and effectively” (3.1).
   c) Process activities.
   d) Roles activities.

10. Syllabus Topic: 4.2
    Correct Answer: B
    Assessment Criteria: Identify cyber resilience activities that should be aligned with IT service strategy (4.2 bulleted list before 4.2.1).

    a) Defining roles for cyber resilience teams is not a part of aligning a cyber resilience strategy with the IT service strategy. Designing cyber resilience would consider the organizational roles needed to meet the strategic objectives.
    b) Understanding business requirements for cyber resilience needs to be aligned to the overall IT service strategy to ensure no conflict and common synergy (4.2).
    c) While a service catalogue is part of IT service strategy, cyber resilience assets would not be included, except within the context of their capability as a service.
    d) Defining those requirements is part of cyber resilience strategy but it would not be integrated with IT service strategy.

11. Syllabus Topic: 4.3 b)
    Correct Answer: D
    Objective: Describe the purpose and key features of the control objectives: manage stakeholders (4.1.2).

    a) Would not be considered typical of a stakeholder category.
    b) Would not be considered typical of stakeholder category.
    c) Would not be considered typical of stakeholder category.
    d) The correct categories are: owners and investors, customers and clients, suppliers, employees, legal and regulatory authorities and competitor and industry bodies (4.1.2.1).

12. Syllabus Topic: 4.3 d)
    Correct Answer: D
    Objective: Describe the purpose and key features of the control objectives: manage audit and compliance (4.1.4).

    a) Is an internal audit activity.
    b) Is an internal audit activity.
    c) Is an internal audit activity.
    d) Is an external audit activity to independently confirm that internal audits have been done appropriately (4.1.4).

13. Syllabus Topic: 4.3 a)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: establish governance (4.1.1 up to but not including 4.1.1.1).

    a) System acquisition and development only addresses control for part of a lifecycle.
    b) This is part of the access control objective of within cyber resilience operation.
    c) Control performance evaluation is a control objective of audit and compliance.
    d) Correct.

14. Syllabus Topic: 4.3 d)
    Correct Answer: B
    Assessment Criteria: Describe the purpose and key features of the control objectives: manage audit and compliance (4.1.4).

    Options A, C and D are all valid types of service and project management related information but would not be typical of cyber resilience compliance evidence. System logs, device logs and transaction logs are essential evidence of how cyber controls are operating.

15. Syllabus Topic: 4.4 c)
    Correct Answer: C
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: financial management for IT Services (4.2.3 including Fig. 4.4).

    Financial management helps quantify the value that IT services contribute to the business and should include cyber-resilience aspects (4.2.3).

16. Syllabus Topic: 5.1
    Correct Answer: B
    Assessment Criteria: Identify what cyber resilience design is intended to achieve (5.0 up to and not including 5.1.1).

    a) An activity of cyber resilience strategy.
    b) B is described as an aspect of cyber resilience design in section 5.0 which says “Cyber Resilience design identifies: how information will be classified and what controls are required for each classification”.
    c) An aspect of cyber resilience transition.
    d) An aspect of cyber resilience transition.

17. Syllabus Topic: 5.3 b)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: system acquisition, development, architecture and design (5.1.2, 5.1.2.1 excluding Table 5.1, 5.1.2.2 excluding Table 5.2, 5.1.2.3 key message only, 5.1.2.4, 5.1.2.6, 5.1.2.7 key message only, excluding 5.1.2.5).

    a) Key message says “If systems are acquired then the security requirements will still apply and the security requirements should be included in any procurement process” (5.1.2.7).
    b) The publication does not describe a “development process” but even if it did this would not impact development done by a third party.
    c) The demand management process may identify security requirements, but would not ensure that these were included in the systems.
    d) The service level management process may document some security controls, but this is an internal document, not a contract with a third party for provision of systems.

18. Syllabus Topic: 5.3 a)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: human resource security (5.1.1, including 5.1.1.1 and 5.1.1.5, excluding 5.1.1.2, 5.1.1.3 and 5.1.1.4).

    a) Physical security will help to prevent some types of inadvertent disclosure, but not for the most likely events.
    b) Operations security will not impact the behaviour of ordinary users.
    c) Endpoint security will help to prevent some specific types of inadvertent disclosure, for example when a device is lost, but not other types of disclosure, such as discussing confidential information in a public place (or losing the endpoint device in the first place).
    d) “On the other hand, poorly trained and unaware employees can inadvertently disclose information” in its discussion of human resource security. Human resource security should address all aspects of inadvertent disclosure (5.1.1).

19. Syllabus Topic: 5.3 c)
    Correct Answer: C
    Assessment Criteria: Describe the purpose and key features of the control objectives: supplier and 3rd party security (5.1.3.1 first para and key message only, 5.1.3.3, 5.1.3.4 including Best Practice call out box).

    a) A is wrong because it may be impractical to carry out risk assessment and testing for minor suppliers.
    b) B is wrong because there may be a key supplier who is neither new nor an outsourcing supplier.
    c) Best practice call out box says “Ensure key suppliers are included in risk assessments and testing” (5.1.3.4).
    d) D is wrong because there may be a key supplier who is neither new nor an outsourcing supplier.

20. Syllabus Topic: 5.3 d)
    Correct Answer: B
    Assessment Criteria: Describe the purpose and key features of the control objectives: endpoint security (5.1.4).

    a) A is wrong because it does not encrypt storage on the endpoint.
    b) Best practice call out box says “Secure endpoints by encrypting the disk/storage and the connection to the organization’s network” (5.1.4).
    c) C is wrong because they do not encrypt the connection to the network.
    d) D is wrong because they do not encrypt the connection to the network.

21. Syllabus Topic: 5.3 e)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: cryptography (5.1.5 first two paras, 5.1.5.5 key message only (key message appears just before the heading 5.1.5.5), 5.1.5.8 first para, Best practice callout box after 5.1.5.9 and before 5.1.6).

    a) "Use encryption to protect communication over untrusted networks" (5.1.5).
    b) B is wrong because network security management is for managing your own networks, not untrusted public networks.
    c) C is wrong because it is likely to be impractical.
    d) D is wrong because it doesn't protect data on public networks, for which contracts are not usually negotiable.

22. Syllabus Topic: 5.3 f)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: business continuity (5.1.6 whole/including sub sections).

    a) "Have a strategy and a business continuity management (BCM) plan for all critical services that sustain the organization" (5.1.6).
    b) B and C are wrong because BCM should cover both internal and third party services.
    c) B and C are wrong because BCM should cover both internal and third party services.
    d) D is wrong because it is not practical, or affordable, to have a BCM plan for all services.

23. Syllabus Topic: 5.4 d)
    Correct Answer: A
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: availability management (5.2.4 including Fig. 5.8).

    "Many of the plans developed by availability management should be included in cyber resilience controls to help defend against threats and vulnerabilities. These are effectively preventative controls" (5.2.4).

24. Syllabus Topic: 6.1
    Correct Answer: B
    Assessment Criteria: Identify what cyber resilience transition is intended to achieve (6.0 up to and not including 6.1).

    When changes are planned, cyber resilience transition must review changes for impact and asses if the level or type of risk has changed, and if updated security controls are needed. These are all valid transition activities.

    All other answer options are not related to transition or support the review activities needed. A is an output of the design phase, C is related to process design and D is related to operational downtime (6.0).

25. Syllabus Topic: 6.2 e)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: testing (6.1.3 excluding Table 6.3 and references to OWASP).

    While B is not untrue and testing does use scenarios and user stories, as described in option C, the most correct answer is A and focuses on the important message that security testing should be embedded throughout the software development lifecycle (SDLC).

26. Syllabus Topic: 6.2 i)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: Information disposal (6.1.7).

    In order to ensure that information is disposed of securely, the policy will need to outline how the information has been classified and what medium it exists on. These attributes dictate what actions should be taken to dispose of the information.

27. Syllabus Topic: 6.2 a)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: Asset management and configuration management (6.1.1 up to and including bulleted list introduced with the phrase “Key elements in asset management are”).

    Critical assets are the assets, be it information or infrastructure, which keep an organization afloat. Without them organizations would not be able to operate (6.1.1).

28. Syllabus Topic: 6.2 b)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: classification and handling (6.1.1.1 excluding Table 6.2).

    Classification helps to control access to and protect assets from unauthorized persons or systems. It also visually conveys the importance of an asset and the desired protection to its legitimate handlers and processors (6.1.1.1).

29. Syllabus Topic: 6.2 f)
    Correct Answer: B
    Assessment Criteria: Describe the purpose and key features of the control objectives: training (6.1.4).

    All of the elements in B are required. Other answers omit one or more and include things that are only appropriate for some staff (6.1.4).

30. Syllabus Topic: 6.2 g)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: documentation management (6.1.5).

    Business critical documents must be kept up to date and circulations controlled. This ensures incorrect decisions and misconfigurations will not be the result of out of date, uncontrolled information. A provides no protection against accidental disclosure (6.1.5). Documentation is not held in the definitive media library (DML) and simply password protecting a document does not ensure it is accurate and available.

31. Syllabus Topic: 6.3 a)
    Correct Answer: B
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: transition planning and support (6.2.1, including Fig. 6.4).

    Sharing competence in management of organizational change to help ensure the success of cyber resilience project is transition planning and support.

32. Syllabus Topic: 6.3 a)
    Correct Answer: C
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: transition planning and support (6.2.1, including Fig. 6.4).

    A is a contribution from release and deployment management to cyber resilience, B is associated with change management and D is how cyber resilience can help transition planning and support.

33. Syllabus Topic: 7.1
    Correct Answer: A
    Assessment Criteria: Identify what cyber resilience operation is intended to achieve (7.0 up to but not including the bulleted list of control types, 7.1 up to but not including 7.1.1).

    The main goals are to prevent, to detect and to correct (7.0).

34. Syllabus Topic: 7.2 a)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: access control (7.1.1 excluding 7.1.1.9 and 7.1.1.10, but including Key Message after 7.1.1.10).

    All of the alternatives are important to monitor (7.1.1.8). However, "logon authentication" is especially important as repeat failed attempts may point to hacking attempts (7.1.2).

35. Syllabus Topic: 7.2 b)
    Correct Answer: C
    Assessment Criteria: Describe the purpose and key features of the control objectives: network security management (7.1.2 first para and Best Practices only and 7.1.2.3, 7.1.2.4, 7.1.2.5, 7.1.2.6 first para and Best Practices only, 7.1.2.7, 7.1.2.8, 7.1.2.9, 7.1.2.11, excluding 7.1.2.1, 7.1.2.2, 7.1.2.10, and 7.1.2.12).

    Cryptography, wireless access and external network connections are all controls that may be utilized in supporting the users' devices. Remote maintenance is sometimes used to enable support personnel to access users' devices (7.1.2.8).

36. Syllabus Topic: 7.2 c)
    Correct Answer: C
    Assessment Criteria: Describe the purpose and key features of the control objectives: physical security (7.1.3, excluding list of data centre standards in 7.1.3.2).

    The objective of physical security is to ensure an organization's building, offices and data centers etc. is secure from physical infiltration by unauthorized persons. Access to secure areas should be limited (7.1.3.3).

37. Syllabus Topic: 7.2 c)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: physical security (7.1.3, excluding list of data centre standards in 7.1.3.2).

    To ensure the risk of losing sensitive information equipment that contains sensitive information and is carried around should utilize full disk encryption (7.1.3.7).

38. Syllabus Topic: 7.2 e)
    Correct Answer: B
    Assessment Criteria: Describe the purpose and key features of the control objectives: incident management (7.1.5, exclude first key message).

    The initial response should always be to contain the incident to make sure further damage is not caused (7.1.5.5).

39. Syllabus Topic: 7.2 e)
    Correct Answer: A
    Assessment Criteria: Describe the purpose and key features of the control objectives: incident management (7.1.5, exclude first key message).

    a) Is a loss of sensitive information and classifies as a security incident (7.1.5.6).
    b) Is an IT operations incident.
    c) Could be a security incident but it is more likely to be an operational incident caused by poor communication.
    d) Is an operational activity.

40. Syllabus Topic: 7.3 a)
    Correct Answer: B
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: event management (7.2.1, including Fig. 7.3).

    Event management is responsible for “monitoring assets to detect changes in state that may be significant for cyber resilience”.

41. Syllabus Topic: 7.3 f)
    Correct Answer: C
    Assessment Criteria: Identify interactions between the following ITSM processes and cyber resilience: service desk (7.2.6).

    A service desk is responsible for first line investigation and diagnosis of incidents (7.2.6).

42. Syllabus Topic: 8.2
    Correct Answer: B
    Assessment Criteria: Recognize maturity models and their purpose (8.5 up to but not including 8.5.1 onwards)

    Two maturity models that should be considered when planning a cyber resilience project are; ITIL process maturity framework and NIST cyber security framework. The Deming cycle and the continual service improvement approach cannot be used as maturity models (8.5).

43. Syllabus Topic: 8.3 a)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: audit and review (8.1.1).

    a) Might be true, but not the main reason.
    b) The controls should support the strategy, not the other way around.
    c) An unlikely output of the review and is not the main purpose.
    d) “The cyber risk landscape is ever evolving and changing. Every day hundreds of new vulnerabilities are discovered” (8.1.1).

44. Syllabus Topic: 8.3 b)
    Correct Answer: C
    Assessment Criteria: Describe the purpose and key features of the control objectives: control assessment (8.1.2).

    The wrong answers refer to technical controls (8.1.2).

45. Syllabus Topic: 8.3 d)
    Correct Answer: B
    Assessment Criteria: Describe the purpose and key features of the control objectives: business continuity improvements (8.1.4).

    Training requirements are a possible output of a post-incident review. An incident is unlikely to directly identify issues with the strategy, risk method or service catalogue (8.1.4.1).

46. Syllabus Topic: 8.3 f)
    Correct Answer: C
    Assessment Criteria: Describe the purpose and key features of the control objectives: remediation and improvement planning (8.1.6, 8.1.6.1 excluding bulleted list and table, 8.1.6.2).

    A cost benefit analysis is a primary input to selecting improvements (8.1.6.2).

47. Syllabus Topic: 8.3 f)
    Correct Answer: D
    Assessment Criteria: Describe the purpose and key features of the control objectives: remediation and improvement planning (8.1.6, 8.1.6.1 excluding bulleted list and table, 8.1.6.2).

    “The findings of the audit and review should be recorded in a suitable manner for the target audience” (8.1.6). The wrong answers take the opposite approach.

48. Syllabus Topic: 8.4
    Correct Answer: B
    Assessment Criteria: Describe how the seven-step improvement process can be used to plan cyber resilience improvements (8.2.3).

    Step 6 box (8.2.3).

49. Syllabus Topic: 8.5
    Correct Answer: C
    Assessment Criteria: Describe how to use ITIL CSI approach to plan cyber resilience improvements (8.3).

    The purpose of the “How do we keep the momentum going?” step for cyber resilience improvement (8.3.6).

50. Syllabus Topic: 9.1
    Correct Answer: C
    Assessment Criteria: Describe segregation of duties and dual controls (9.2).

    Nobody should authorize or audit his own access. Table 9.3 shows this specific violation as an example.