RESILIA™ Practitioner Examination Syllabus

V1.0

August 2015

AXELOS.com

RESILIA Practitioner Examination Syllabus

The table below specifies the learning outcomes of the RESILIA Practitioner qualification and the minimum course content for each learning outcome as referenced to the RESILIA™: Cyber Resilience Best Practice publication. It also specifies the assessment criteria used to assess candidate's achievement of the learning outcomes subsequent to attending the course.

The examination duration is 2 hours and 15 minutes. Candidates are expected to achieve a score of TBC% or higher in order to pass the examination and be awarded certification.

Learning Outcomes	Assessment Criteria (references to the RESILIA™: Cyber Resilience Best Practice publication in brackets) The verb for each assessment criteria indicates the Bloom's level: e.g. 'Describe', 'Explain', 'Distinguish' indicates Level 2 understanding/comprehension e.g. 'Solve', 'Calculate', 'Apply', 'Work Out' indicates Level 3 (Application - Carry out or use a procedure in a given situation)	Bloom's Level	No. of qsts	Exam Weight (%)	Exam sections
1. Be able to carry out risk management	1.1 Distinguish between the terms: risk, asset, vulnerability, threat (2.2)	2	1	16	8 x MCQ questions on one scenario
	1.2 Determine the actions needed to address risks and opportunities and explain their purpose (2.3): a) Establish context (2.3.1) b) Establish criteria for risk assessment and acceptance (2.3.2) c) Risk identification (2.3.3) d) Risk analysis and evaluation (2.3.4) e) Risk treatment (2.3.5, 4.2.6) i) Risk avoidance (2.3.5.1) ii) Risk modification (2.3.5.2) iii) Risk sharing (2.3.5.3) iv) Risk retention (2.3.5.4) f) Risk monitoring and review (2.3.6)	3	5		
	1.3 Create and manage a: a) Risk register (2.3.3) b) Risk treatment plan (2.3.5)	3	2		

2. Be able to manage the controls relevant to cyber resilience strategy and align these with IT service management	2.1 Explain the purpose and use of the control objectives (4.1): a) Establish governance (4.1.1) i) vision and mission (4.1.1.1) ii) key activities (Fig 4.1/4.1.1) b) Manage stakeholders (4.1.2) c) Identify and categorize stakeholders (4.1.2.1) i) gather stakeholder requirements (4.1.2.2) ii) plan communication (4.1.2.3 excluding content of strategic communication plan) d) Create and manage cyber resilience policies (4.1.3, not including bulleted list of policies) i) structure of cyber resilience policies (4.1.3.1) ii) management of cyber resilience policies (4.1.3.2) e) Manage audit and compliance (4.1.4) i) audit (4.1.4.1) ii) compliance management (4.1.4.2)	3	5	16	8 x MCQ questions on one scenario
	2.2 Explain how ITSM processes and cyber resilience interact (4.2.7): (knowledge of the underlying ITSM processes will not be examined) a) Strategy management for IT Services (4.2.1) b) Service portfolio management (4.2.2, including Fig. 4.3) c) Financial management for IT Services (4.2.3) d) Demand management (4.2.4) e) Business relationship management (4.2.5) f) Information risk management and risk treatment (4.2.6)	3	3		
3. Be able to manage the controls relevant to cyber resilience design and align these with IT service management	3.1 Explain the purpose and use of the control objectives (5.1): a) Human resource security (5.1.1 including all sub-sections) b) 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) c) Supplier and 3rd party security (5.1.3.1, 5.1.3.2, 5.1.3.3, 5.1.3.4 including Best Practice call out box) d) Endpoint security (5.1.4) e) Cryptography (5.1.5 first two paras, 5.1.5.4 key message only, 5.1.5.5 Best Practice call out box	3	6	18	9 x MCQ questions on one scenario

	only, 5.1.5.7 first para) f) Business continuity (5.1.6 whole/including sub sections)				
	3.2 Explain how ITSM processes and cyber resilience interact (5.2.9): (knowledge of the underlying ITSM processes will not be examined) a) Design co-ordination (5.2.1 including Fig. 5.5) b) Service catalogue management (5.2.2 including Fig. 5.6) c) Service level management (5.2.3 including Fig. 5.7) d) Availability management (5.2.4 including Fig. 5.8) e) Capacity management (5.2.5 including Fig. 5.9) f) IT service continuity management (5.2.6 including Fig. 5.10) g) Supplier management (5.2.7 including Fig. 5.11)	3	3		
4. Be able to manage the controls relevant to cyber resilience transition and align these with IT service management	4.1 Explain the purpose and use of the control objectives (6.1): a) Asset management and configuration management (6.1.1) b) Classification and handling (6.1.1.1, excluding Table 6.2) c) Data transportation and removable media (6.1.1.2) d) Change management (6.1.2 excluding bulleted list introduced with the phrase “ITIL change management for instance helps;”) e) Testing (6.1.3 excluding Table 6.3 & references to OWASP) f) Training (6.1.4) g) Documentation management (6.1.5) h) Information retention (6.1.6 first two paras) i) Information disposal (6.1.7)	3	6	18	9 x MCQ questions on one scenario

	4.2 Explain how ITSM processes and cyber resilience interact (6.2): (knowledge of the underlying ITSM processes will not be examined) a) Transition planning and support (6.2.1) b) Change management (6.2.2) c) Service asset and configuration management (6.2.3) d) Release and deployment management (6.2.4) e) Service validation and testing (6.2.5) f) Change evaluation (6.2.6) g) Knowledge management (6.2.7) h) Management of organizational change (6.2.8)	3	3		

5. Be able to manage the controls relevant to cyber resilience operation and align these with IT service management	5.1 Explain the purpose and use of the control objectives (7.1): a) Access control (7.1.1 excluding 7.1.1.9 and 7.1.1.10) b) Network security management (7.1.2 first para and Best Practices only & 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) c) Physical security (7.1.3, excluding list of data centre standards in 7.1.3.2) d) Operations security (7.1.4, excluding 7.1.4.1) e) Incident management (7.1.5, exclude first key message)	3	5	16	8 x MCQ questions on one scenario
	5.2 Explain how ITSM processes and cyber resilience interact (7.2.10): (knowledge of the underlying ITSM processes will not be examined) a) Event management (7.2.1) b) Incident management (7.2.2) c) Request fulfilment (7.2.3) d) Problem management (7.2.4) e) Access management (7.2.5) f) Service desk (7.2.6) g) Technical management (7.2.7) h) Application management (7.2.8) i) IT operations management (7.2.9)	3	3		
6. Be able to manage the controls relevant to cyber resilience continual improvement and align these with IT service management	6.1 Explain the purpose and use of the control objectives (8.1): a) Audit and review (8.1.1) b) Control assessment (8.1.2) c) Key Performance Indicators (KPI), Key Risk Indicators (KRI), Benchmarking (8.1.3 Excluding tables) d) Business continuity improvements (8.1.4) e) Process improvements (8.1.5) f) Remediation and improvement planning (8.1.6 excluding bulleted list and table, 8.1.6.1)	3	4	14	7 x MCQ questions on one scenario
	6.2 Apply the seven-step improvement process to plan cyber resilience improvements (8.2.3)	3	2		
	6.3 Apply the ITIL CSI approach to cyber resilience (8.3)	3	1		

7. Be able to evaluate need for segregation of duties and dual controls	7.1 Apply the concepts of segregation of duties and dual controls to an organizational context (9.2)	3	1	2	1 x MCQ questions on one scenario
TOTAL			50	100	