Cyber Resilience – draft Foundation syllabus (exam duration =100 minutes)

Learning Outcomes	Assessment criteria The verb for each syllabus area/assessment criteria indicates the Bloom's level: e.g. 'Identify', 'Recall', 'Recognise' indicates Level 1 basic recall and recognition & e.g. 'Describe', 'Explain', 'Distinguish' indicates Level 2 understanding/comprehension	Blooms Level	No. of qsts	Question type	Exam Weighting
1. Intro to Cyber Resilience *Understand the purpose, benefits and key terms of cyber resilience*	1.1 Describe what cyber resilience is (1.4.5)	Inferred knowledge			2 (4 %)
	1.2 Identify the benefits of cyber resilience (1.3/1.4/1.6)				
	1.3 Identify the terms a) security and resilience (1.4.4) b) preventative detective, and corrective controls (1.4.6/1.5.7) c) people, process and technology (1.7.3)	1	1	MC standard	
	1.4 Identify the purpose of balancing *a) preventative detective, and corrective controls (1.4.6/1.5.7)* *b) people, process, technology (1.7.3)* *c) risks and opportunities (1.5.1)*	2	1	MC standard	
	1.5 Identify the need for: *a) Confidentiality (1.5.5)* *b) Integrity (1.5.5)* *c) Availability (1.5.5)* *d) Authentication (1.5.6)* *e) Nonrepudiation (1.5.6)*				
2. Risk management *Understand the purpose of risk management and the key activities needed to address risks and opportunities*	2.1 Describe what risk management is (2.0 up to but not including 2.1 onwards)	2	1	MC standard	5 (10 %)
	2.2 Identify the purpose of risk management	2			
	2.3 Identify the terms: risk, asset, vulnerability, threat (2.2)	1	1	MC standard	
	2.4 Describe actions to address risks and opportunities:(2.3) *a) Establish context* *b) Establish criteria for risk assessment and acceptance* *c) Risk identification* *d) Risk analysis and evaluation* *e) Risk treatment* *f) Risk monitoring and review*	2	2	MC standard	

	2.5 Identify the terms: *a) Risk register (2.3.3)* *b) Risk avoidance(2.3.5)* *c) Risk modification (2.3.5)* *d) Risk sharing (2.3.5)* *e) Risk retention (2.3.5)* *f) Risk treatment plan (2.3.5)* *g) Defence-in-depth (2.3.5)*	1	1	MC standard	
3. Managing Cyber Resilience *Understand the purpose of a management system and how best practices and standards can contribute*	3.1 Identify the purpose and scope of a management system (3.1)	1	1	MC standard	2 (4 %)
	3.2 Identify the components of a management system (first bulleted list in 3.1)	1			
	3.3 Recognize the relevance of common management standards and best practice frameworks to cyber resilience (3.1) *a) ITIL (3.1.1)* *b) ISO/IEC 27001 (3.1.2)* *c) NIST Framework for Improving Critical Infrastructure Cybersecurity (8.5.2 up to but not including 8.5.2.1)*	1			
	3.4 Describe the difference between management, governance (3.1) and compliance (4.1.4.2)	2	1	MC standard	
4. Cyber Resilience Strategy *Understand the purpose of cyber resilience strategy, the associated control objectives and their interactions with ITSM activities*	4.1 Identify what cyber resilience strategy is intended to achieve (Section 4 up to and not including 4.1.1)	1	1	MC standard	6 (12 %)
	4.2 Identify cyber resilience activities that should be aligned with IT service strategy (4.2 bulleted list before 4.2.1)	1			

	4.3 Describe the purpose and key features of the control objectives: *a) establish governance (4.1.1 up to but not including 4.1.1.1)* *i) key activities (Fig 4.1/4.1.1)* *b) manage stakeholders (4.1.2)* *i) common categories (4.1.2.1)* *ii) gathering requirements (4.1.2.2 bulleted list only)* *iii) planning communication (4.1.2.3 excluding content of strategic communication plan)* *c) create and manage policies (4.1.3 up to but not including 4.1.3.1, not including bulleted list of policies, including 4.1.3.2)* *d) manage audit and compliance (4.1.4)*	2	4	MC standard	
	4.4 Identify interactions between the following ITSM processes and cyber resilience: *(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 including Fig. 4.4)* *d) Demand management (4.2.4 including Fig. 4.5)* *e) Business Relationship Management (4.2.5)*	1	1	MC standard	
5. Cyber Resilience Design *Understand the purpose of cyber resilience design, the associated control objectives and their interactions with ITSM activities*	5.1 Identify what cyber resilience design is intended to achieve (Section 5 up to and not including 5.1.1)	1	1	MC standard	8 (16 %)
	5.2 Identify cyber resilience activities that should be aligned with IT service design (5.2 bulleted list before 5.2.1)	1			
	5.3 Describe the purpose and key features of the control objectives: *a) 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)* *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 first para & key message only, 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, 5.1.5.5 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)* *f) Business continuity (5.1.6 whole/including sub sections)*	2	6	MC standard	
	5.4 Identify interactions between the following ITSM processes and cyber resilience: *(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)*	1	1	MC standard	

	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)*				
6. Cyber Resilience Transition *Understand the purpose of cyber resilience transition, the associated control objectives and their interactions with ITSM activities*	6.1 Identify what cyber resilience transition is intended to achieve (Section 6 up to and not including 6.1.1)	1	1	MC standard	9 (18 %)
	6.2 Describe the purpose and key features of the control objectives: *a) Asset management and configuration management (6.1.1 up to and including bulleted list introduced with the phrase "Key elements in asset management are:")* *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 "For instance, ITIL change management helps to:")* *e) Testing (6.1.3 excluding Table 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)*	2	6	MC standard	
	6.3 Identify interactions between the following ITSM processes and cyber resilience: *(knowledge of the underlying ITSM processes will not be examined)* *a) Transition planning and support (6.2.1, including Fig. 6.4)* *b) Change management (6.2.2, including Fig. 6.5)* *c) Service asset and configuration management (6.2.3, including Fig. 6.6)* *d) Release and deployment management (6.2.4, including Fig. 6.7)* *e) Service validation and testing (6.2.5, including Fig. 6.8)* *f) Change evaluation (6.2.6, including Fig. 6.9)* *g) Knowledge management (6.2.7)* *h) Management of organizational change (6.2.8)*	1	2	MC standard	
7. Cyber Resilience Operation *Understand the purpose of cyber resilience operation, the associated control objectives and their interactions with ITSM activities*	7.1 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)	1	1	MC standard	9 (18%)
	7.2 Describe the purpose and key features of the control objectives : *a) Access control (7.1.1 excluding 7.1.1.9 and 7.1.1.10, but including Key Message after 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)*	2	4	MC standard	
	e) Incident management (7.1.5, exclude first key message)	2	2	MC standard	

	7.3 Identify interactions between the following ITSM processes and cyber resilience: *(knowledge of the underlying ITSM processes will not be examined)* *a) Event management (7.2.1, including Fig. 7.3)* *b) Incident management (7.2.2, including Fig. 7.4)* *c) Request fulfilment (7.2.3, including Fig. 7.5)* *d) Problem management (7.2.4, including Fig. 7.6)* *e) Access management (7.2.5, including Fig. 7.7)* *f) Service desk (7.2.6)* *g) Technical management (7.2.7)* *h) Applications management (7.2.8)* *i) IT operations management (7.2.9)*	1	2	MC standard	
8. Cyber Resilience Continual Improvement *Understand the purpose of cyber resilience continual improvement, the associated control objectives and their interactions with ITSM activities*	8.1 Identify what cyber resilience continual improvement is intended to achieve (Section 8 up to but not including 8.1.1)	1	1	MC standard	8 (16 %)
	8.2 Recognise maturity models and their purpose *(8.5 up to but not including 8.5.1 onwards)*	1			
	8.3 Describe the purpose and key features of the control objectives:				
	a) Audit and review (8.1.1)	2	1	MC standard	
	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, 8.1.6.1 excluding bulleted list and table, 8.1.6.2)*	2	4	MC standard	
	8.4 Describe how the seven-step improvement process can be used to plan cyber resilience improvements *(8.2.3)*	2	1	MC standard	
	8.5 Describe how to use ITIL CSI approach to plan cyber resilience improvements *(8.3)*	2	1	MC standard	
9. Cyber Resilience Roles & responsibilities *Understand the purpose and benefits of segregation of duties and dual controls*	9.1 Describe segregation of duties and dual controls *(9.2)*	2	1	MC standard	1 (2 %)
TOTAL			**50**		**100 %**