ID	Objective	Module	Page in 07 Module Specification and Module Delivery details
K1	Principles of networks: OSI and TCP/IP models, data, protocols and how they relate to each other; the main routing protocols; the main factors affecting network performance including typical failure modes in protocols and approaches to error control; virtual networking	NCS101	20
K2	the concepts, main functions and features of at least three Operating Systems (OS) and their security functions and associated security features	NCS204	61
K3	Cyber security concepts and why cyber security matters to business and society; Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods	NCS204	61
K4	the main types of common attack techniques; also the role of human behaviour, including the significance of the 'insider threat'. Including: - how attack techniques combine with motive and opportunity to become a threat. - techniques and strategies to defend against attack techniques and mitigate hazards	NCS204	61
K5	the significance of identified trends in cyber security threats and understand the value and risk of this analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment.	NCS204	61
K6	lifecycle and service management practices to an established standard to a foundation level for example Information Technology Infrastructure Library (ITIL) foundation level.	WRL100\NCS101	7/20
K7	cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.	NCS104	36
K8	Understands the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. To include: laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation); use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions..	NCS104	36
K9	ethical principles and codes good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional.	NCS104	36
K10	how to analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification	WRL100\NCS201	16/49
K11	horizon scanning including use of recognised sources of threat intelligence and vulnerabilities.	NCS204	61
K12	common security architectures and methodologies; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. How cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls.	NCS202	53
K13	the basic terminology and concepts of cryptography; common cryptography techniques in use; the importance of effective key management and the main techniques used; legal, regulatory and export issues specific to use of cryptography.	NCS103\NC203	30/57
K14	risk assessment and audit methodologies and approaches to risk treatment; approaches to identifying the vulnerabilities in organisations and security management systems; the threat intelligence lifecycle; the role of the risk owner in contrast with other stakeholders	WRL100	16
K15	principles of security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes.	NCS201\WRL100	16/49
K16	function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security	NCS202\NCS204	53/61
K17	programming or scripting languages	NCS103\NCS203	30/57
S1	Discover vulnerabilities in a system by using a mix of research and practical exploration).	NCS204	61
S2	Analyse and evaluate security threats and hazards to a system or service or processes. Use relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) Combine different sources to create an enriched view of cyber threats and hazards.	NCS204\WKL200	44/61
S3	Research and investigate common attack techniques and relate these to normal and observed digital system behaviour and recommend how to defend against them. Interpret and demonstrate use of external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source).	NCS104\NCS204	35/61
S4	Undertake security risk assessments for simple systems without direct supervision and propose basic remediation advice in the context of the employer.	NCS204	61
S5	Source and analyse security cases and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern	NCS204\WKL200	44/61
S6	Analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification	NCS201\WRL100\WKL200	16/44/49
S7	Identify and follow organisational policies and standards for information and cyber security and operate according to service level agreements or other defined performance targets.	WRL100\WKL200	16/44
S8	Configure, deploy and use computer, digital network and cyber security technology.	All modules	
S9	Recommend improvements to the cyber security posture of an employer or customer based on research into future potential cyber threats and considering threat trends.	NCS204\WKL200	44/61
S10	Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to a given design requirement without supervision. Provide evidence that the system meets the design requirement.	NCS101, NCS201\NCS202	20/50/53
S11	Analyse security requirements (functional and non-functional security requirements that may be presented in a security case) against other design requirements (e.g. usability, cost, size, weight, power, heat, supportability etc.), given for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.	WRL100\WKL200	16/44
S12	Design and build, systems in accordance with a security case within broad but generally well-defined parameters. This should include selection and configuration of typical security hardware and software components. Provide evidence that the system has properly implemented the security controls required by the security case	WKL200\NCS201	44/49
S13	Write program code or scripts to meet a given design requirement in accordance with employers' coding standards.	NCS103\NCS203	30/57
S14	Design systems employing encryption to meet defined security objectives. Develop and implement a plan for managing the associated encryption keys for the given scenario or system.	NCS201 & NCS103	49/30
S15	Use tools, techniques and processes to actively prevent breaches to digital system security.	NCS202	53
S16	Conduct cyber-risk assessments against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.	CMP204	61
S17	Identify cyber security threats relevant to a defined context	CMP204\WKL200	44/61
S18	Develop information security policies or processes to address a set of identified risks, for example from security audit recommendations.	CMP204\WRL100\WKL200	16/44/61
S19	Develop information security policies within a defined scope to take account of legislation and regulation relevant to cyber security	NCS204\NCS201\WKL200	44/49/61
S20	Take an active part in a security audits against recognised cyber security standards, undertake gap analysis and make recommendations for remediation.	NCS204	61
S21	Develop plans for incident response for approval within defined governance arrangements for incident response.	WRL100\WKL200	16/44
S22	Develop plans for local business continuity for approval within defined governance arrangements for business continuity.	WRL100\WKL200	16/44
S23	Assess security culture using a recognised approach.	WRL100\WKL200	16/44
S24	Design and implement a simple ‘security awareness’ campaign to address a specific aspect of a security culture.	PFD200	39
S25	Integrate and correlate information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach	WKL200	44
S26	Recognise anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.	NCS204	61
S27	Accurately, objectively and concisely record and report the appropriate cyber security information, including in written reports within a structure or template provided.	WRL100\WKL200\NCS204	16/44/61
S28	Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise.	NCS204	61
S29	Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.	NCS204	61
S30	Manage local response to non-major incidents in accordance with a defined procedure.	WRL100\WKL200	16/44
B1	Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B2	Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions.	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B3	Works independently and takes responsibility. For example, works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B4	Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B5	Thorough & organised. For example uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B6	Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B7	Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B8	Maintains a productive, professional and secure working environment.	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B9	Creative - taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec
B10	: Problem Solving - Identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence.	See page 29 of 05. Programme Spec	See page 29 of 05. Programme Spec

Note: All module specs can be found in 7. Module Specification and Module Delivery details

ID	Objective	Module	Page in 07 Module Specification and Module
K1	the causes and consequences of network and IT infrastructure failures	NCS101	20
K2	the architecture of typical IT systems, including hardware, OS, server, virtualisation, voice, cloud, and applications	NCS101\NCS201	20/49
K3	the techniques for systems performance and optimisation	NCS201\NCS202	49/53
K4	diagnostic techniques and tools to interrogate and gather information regarding systems performance	NCS202\NCS201	49/53
K5	organizational procedures to deal with recording information effectively and in line with protocols	WRL100	16
K6	Service Level Agreements (SLAs) and their application to delivering network engineering activities in line with contractual obligations and customer service	WRL100	16
K7	their role in Business Continuity and Disaster Recovery	WRL100	16
K8	the purposes and uses of ports and protocols	NCS101\NCS201	20/49
K9	devices, applications, protocols, and services at their appropriate OSI and/or TCP/IP layers.	NCS101	20
K10	the concepts and characteristics of routing and switching	NCS101	20
K11	the characteristics of network topologies, types, and technologies.	NCS101	20
K12	wireless technologies and configurations.	NCS201	49
K13	cloud concepts and their purposes.	NCS201	49
K14	functions of network services	NCS201	49
K15	the different types of network maintenance	WRL100\WKL200	16/44
K16	how current legislation relates to or impacts occupation	NCS104	35
K17	troubleshooting methodologies for network and IT infrastructure	NCS101	20
K18	how to integrate a server into a network	NCS201	49
K19	the types of security threats to networks and IT infrastructure assets	NCS204	61
K20	how to use tools to automate network tasks	NCS201	49
K21	approaches to change management	WKL200	44
S1	apply the appropriate tools and techniques when securely operating and testing Networks	NCS201\NCS202\NCS204	49/53/61
S2	install and configure the elements required to maintain and manage a secure Network	NCS201\NCS202	49/53
S3	implement techniques to monitor and record systems performance in line with defined specifications	NCS201\NCS202	49/53
S4	maintain security and performance of the system against known and standard threats	NCS204	61
S5	apply the appropriate tools and techniques to identify systems performance issues	NCS201\202	49/53
S6	apply the appropriate tools and techniques to gather information to troubleshoot issues and isolate, repair or escalate faults	NCS101\NCS201	20/49
S7	communicate outcomes of tasks and record in line with organisational procedures and SLAs including adherence to good customer service standards	WRL100\WKL200	16/44
S8	upgrade, apply and test components to systems configurations ensuring that the system meets the organisation's requirements and minimises downtime. This should include backup processes.	NCS202\WKL200	53/44
S9	record task details whether face-to-face, remote or in writing in line with ogranisational requirements	WRL100\NCS101	16/20
S10	interpret information received from a manager, customer or technical specialist and accurately implement the defined requirements	NCS201	49
S11	monitor, identify and implement required maintenance procedures	NCS101\NCS201	20/49
S12	implement techniques to optimise systems performance in line with defined specifications	NCS102	25
S13	organise and prioritise clients/stakeholders' requests in line with SLAs and organization processes	WRL100\WKL200	16/44
S14	explain their job role within the business context to stakeholders to enable a clear understanding on both sides of what their remit is and convey technical constraints in appropriate language considering accessibility and diversity implications.	WRL100\WKL200\PFD200	16/44/40
S15	operate securely and apply the appropriate process, policies, and legislation within their business responsibilities	NCS201	49
S16	communicate with a range of stakeholders taking into consideration of organisations cultural awareness and technical ability	WRL100\WKL200	16/44
S17	apply the appropriate level of responsibility when planning and prioritizing work tasks	PFD200	39
S18	apply the relevant numerical skills (Binary, dotted decimal notation) required to meet the defines specifications	NCS101	20
S19	ensure compliance of network engineering outputs with change management processes	WRL\WKL200	16/44
S20	select the appropriate tools and comply with organisation policies and processes when upgrading systems	NCS101\NCS102\NCS201\NCS202	20/25/49/53
B1	work independently and demonstrate initiative being resourceful when faced with a problem and taking responsibility for solving problems within their own remit	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B2	work securely within the business	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B3	work within the goals, vision, and values of the organisation	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B4	take a wider view of the strategic objectives of the tasks/ projects they are working on including the implications for accessibility by users and diversity.	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B5	works to meet or exceed customers' requirements and expectations	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B6	Identifies issues quickly, investigates and solves complex problems and applies appropriate solutions. Ensures the true root cause of any problem is found and a solution is identified which prevents recurrence	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B7	Committed to continued professional development to ensure growth in professional skill and knowledge.	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec
B8	work effectively under pressure showing resilience	See Page 30 of 05. Programme Spec	See Page 30 of 05. Programme Spec

Note: All module specs can be found in 7. Module Specification and Module Delivery details