Level 5 Extended Diploma in Networking and Cyber Security (610/3042/9)

Qualification Specification

September 2023

Contents

About QUALIFI

QUALIFI is recognised and regulated by Ofqual (Office of Qualifications and Examinations Regulator). Our Ofqual reference number is RN5160. Ofqual regulates qualifications, examinations, and assessments in England.

As an Ofqual recognised Awarding Organisation, QUALIFI is required to carry out external quality assurance to ensure that centres approved for the delivery and assessment of QUALIFI's qualifications meet the required standards.

Why Choose QUALIFI Qualifications?

QUALIFI qualifications aim to support learners to develop the necessary knowledge, skills and understanding to support their professional development within their chosen career and or to provide opportunities for progression to further study.

Our qualifications provide opportunities for learners to:

- apply analytical and evaluative thinking skills
- develop and encourage problem solving and creativity to tackle problems and challenges
- exercise judgement and take responsibility for decisions and actions
- develop the ability to recognise and reflect on personal learning and improve their personal, social, and other transferable skills.

Employer Support for the Qualification Development

During the development of this qualification QUALIFI consults a range of employers, providers, and existing centres (where applicable) to ensure rigour, validity and demand for the qualification and to ensure that the development considers the potential learner audience for the qualification and assessment methods. The qualification is not intended to be a licence to offer financial advice. Learners should seek further certification in this case.

Equality and Diversity

QUALIFI's qualifications are developed to be accessible to all learners who are capable of attaining the required standard. QUALIFI promotes equality and diversity across aspects of the qualification process and centres are required to implement the same standards of equal opportunities and ensure teaching and learning are free from any barriers that may restrict access and progression.

Learners with any specific learning need should discuss this in the first instance with their approved centre who will refer to QUALIFI's Reasonable Adjustment and Special Consideration Policy.

Qualification Title and Accreditation Number

This qualification has been accredited to the Regulated Qualification Framework (RQF) and has its own unique Qualification Accreditation Number (QAN). This number will appear on the learner's final certification document. Each unit within the qualification has its own RQF code. The QAN for this qualification is as follows:

Qualifi Level 5 Extended Diploma in Networking and Cyber Security

(610/3042/9)

Qualification Aims and Learning Outcomes

Aim of the QUALIFI Level 5 Extended Diploma in Networking and Cyber Security

The aim of the QUALIFI Level 5 Extended Diploma in Networking and Cyber Security is to provide learners with an extended range of understanding of networking and cybersecurity.

The units for this qualification have been taken from existing Qualifi qualifications:

Qualifi Level 4 Diploma in Cyber Security (603/3331/5)

Qualifi Level 4 Diploma in IT – Networking (603/4782/X)

Qualifi Level 5 Diploma in Cyber Security (603/4139/7)

Qualifi Level 5 Diploma in IT – Networking (603/4792/2)

It is envisaged that learners who successfully complete this qualifications will have gained a broader understanding of cyber scurity and how to implement networking systems to remove any such risks.

Successful completion of the QUALIFI Level 5 Extended Diploma in Networking and Cyber Security provides learners with the opportunity to progress to further study or employment.

Learning Outcomes of the QUALIFI Level 5 Extended Diploma in Networking and Cyber Security

All learning outcomes and assessment criteria for each unit are outlined in the unit specifications.

Delivering the Qualification

External Quality Assurance Arrangements

All centres are required to complete an approval process to be recognised as an approved centre. Centres must have the ability to support learners. Centres must commit to working with QUALIFI and its team of External Quality Assurers (EQAs). Approved centres are required to have in place qualified and experienced tutors and all tutors are required to undertake regular continued professional development (CPD).

Approved centres will be monitored by QUALIFI External Quality Assurers (EQAs) to ensure compliance with QUALIFI requirements and to ensure that learners are provided with appropriate learning opportunities, guidance and formative assessment.

QUALIFI's guidance relating to invigilation, preventing plagiarism and collusion will apply to centres.

Unless otherwise agreed, QUALIFI:

- sets all assessments.
- moderate's assessments prior to certification.
- awards the final mark and issues certificates.

Learner Induction and Registration

Approved centres should ensure all learners receive a full induction to their study programme and the requirements of the qualification and its assessment.

All learners should expect to be issued with the course handbook and a timetable and meet with their personal tutor and fellow learners. Centres should assess learners carefully to ensure that they are able to meet the requirements qualification and that, if applicable, appropriate pathways or optional units are selected to meet learners' progression requirements.

Centres should check the qualification structures and unit combinations carefully when advising learners. Centres will need to ensure that learners have access to a full range of information, advice and guidance to support them in making the necessary qualification and unit choices. During recruitment, approved centres need to provide learners with accurate information on the title and focus of the qualification for which they are studying.

All learners must be registered with QUALIFI within the deadlines outlined in the QUALIFI Registration, Results and Certification Policy and Procedure.

Entry Criteria

Approved centres are responsible for reviewing and making decisions as to an applicant's ability to complete the learning programme successfully and meet the demands of the qualification. The initial assessment by the centre will need to consider the support that is readily available or can be made available to meet individual learner needs as appropriate.

The qualification has been designed to be accessible without artificial barriers that restrict access. For this qualification, applicants must be aged 18 or over.

In the case of applicants whose first language is not English, then IELTS 6 (or equivalent) is required. International qualifications will be checked for appropriate enrolment to UK higher education postgraduate programmes where applicable. Applicants are normally required to produce two supporting references, at least one of which should preferably be academic.

Recognition of Prior Learning

Recognition of Prior Learning (RPL) is a method of assessment (leading to the award of credit) that considers whether learners can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and so do not need to develop through a course of learning.

QUALIFI encourages centres to recognise learners' previous achievements and experiences whether at work, home or at leisure, as well as in the classroom. RPL provides a route for the recognition of the achievements resulting from continuous learning. RPL enables recognition of achievement from a range of activities using any valid assessment methodology. Provided that the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable for accrediting a unit, units, or a whole qualification.

Evidence of learning must be valid and reliable. For full guidance on RPL please refer to QUALIFI's *Recognition of Prior Learning Policy*.

Data Protection

All personal information obtained from learners and other sources in connection with studies will be held securely and will be used during the course and after they leave the course for a variety of purposes and may be made available to our regulators. These should be all explained during the enrolment process at the commencement of learner studies. If learners or centres would like a more detailed explanation of the partner and QUALIFI policies on the use and disclosure of personal information, please contact QUALIFI via email support@QUALIFI-international.com

Learner Voice

Learners can play an important part in improving the quality through the feedback they give. In addition to the on-going discussion with the course team throughout the year, centres will have a range of mechanisms for learners to feed back about their experience of teaching and learning.

Professional Development and Training for Centres

QUALIFI supports its approved centres with training relating to our qualifications. This support is available through a choice of training options offered through publications or through customised training at your centre.

The support we offer focuses on a range of issues including:

- planning for the delivery of a new programme.
- planning for assessment and grading.
- developing effective assignments.
- building your team and teamwork skills.
- developing learner-centred learning and teaching approaches.
- building in effective and efficient quality assurance systems.

Please contact us for further information.

Progression and Links to other QUALIFI Programmes

Completing the **QUALIFI Level 5 Extended Diploma in Networking and Cyber Security** will enable learners to progress to:

- QUALIFI Level 6 Diploma.
- University to complete a Degree.
- Employment in an associated profession.

Qualification Structure and Requirements

Credits and Total Qualification Time (TQT)

The QUALIFI Level 5 Extended Diploma in Networking and Cyber Security is made up of 240 credits which equates to hours 2400 of TQT.

Total Qualification Time (TQT) is an estimate of the total amount of time that could reasonably be expected to be required for a learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification.

Examples of activities that can contribute to Total Qualification Time includes guided learning, independent and unsupervised research/learning, unsupervised compilation of a portfolio of work experience, unsupervised e-learning, unsupervised e-assessment, unsupervised coursework, watching a prerecorded podcast or webinar, unsupervised work-based learning.

Guided Learning Hours (GLH) are defined as the time when a tutor is present to give specific guidance towards the learning aim being studied on a programme. This definition includes lectures, tutorials and supervised study in, for example, open learning centres and learning workshops, live webinars, telephone tutorials or other forms of e-learning supervised by a tutor in real time. Guided learning includes any supervised assessment activity; this includes invigilated examination and observed assessment and observed work-based practice.

Rules of Combination for QUALIFI Level 5 Extended Diploma in Networking and Cyber Security

All Units are mandatory.

Unit Reference	Mandatory Units	Level	TQT	Credit	GLH
T/617/1129	Cyber Security Threat and Risk	4	200	20	100
K/617/1130	Network Security and Data Communications	4	200	20	100
M/617/1131	Database Security and Computer Programming	4	200	20	100
T/617/1132	Incident Response, Investigations and Forensics	4	200	20	100
A/617/1133	Security Strategy: Laws, Policies and Implementation	4	200	20	100

Unit Reference	Mandatory Units	Level	TQT	Credit	GLH
K/617/6697	Physical IT Networking	4	200	20	100
J/617/4634	Cryptography	5	300	30	150
L/617/4635	Digital Investigations and Forensics	5	300	30	150
R/617/6743	System Administration	5	200	20	100
Y/617/6744	Network Routing and Switching	5	200	20	100
D/617/6745	Network Design and Administration	5	200	20	100
		Total	**2400**	**240**	**1200**

Achievement Requirements

Learners must demonstrate they have met all learning outcomes and assessment criteria for all the required units to achieve this qualification. QUALIFI will issue certificates to all successful learners via their registered centres.

Awarding Classification/Grading

All unit grading is shown on the qualification transcript.

Fail - 0-39%

Pass - 40%-59%

Merit - 60% - 69%

Distinction 70%+

All units will be internally assessed through written assignment, internally marked by the QUALIFI approved centre and subject to external quality assurance by QUALIFI.

Assessment Strategy and Methods

QUALIFI will provide assessments for each unit of this qualification. These tasks will address all learning outcomes and related assessment criteria, all of which must be demonstrated/passed in order to achieve the qualification.

The tasks will enable learners to draw on work-related information and/or examples wherever possible. Some assessment tasks will contain a practical assignment which will require observation by an assessor (see Assessment Guidance for further information).

The assessment tasks will require learners to draw on real organisational information or case studies to illustrate their answers. To support this activity during the programme of learning, centres are required to make sure that they include case studies of relevant organisations and, wherever possible, encourage learners to draw on work-place opportunities to undertake research and investigation to support their learning.

Learner assessments will be marked internally by the approved centre and will be subject to external moderation by QUALIFI prior to certification.

All learning outcomes and related assessment criteria must be demonstrated/passed in order to achieve the qualification. To achieve a pass for each of the units, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards required for all the assessment criteria.

Qualifi will provide a combination of assessment that cover the learning outcomes and assessment criteria. These may be as follows.

1: Formative Assessment

Formative assessment is an integral part of the assessment process, involving both the tutor/assessor and the learner about their progress during the course of study. Formative assessment takes place prior to summative assessment and focuses on helping the learner to reflect on their learning and improve their performance and does not confirm achievement of grades at this stage.

The main function of formative assessment is to provide feedback to enable the learner to make improvements to their work. This feedback should be prompt so it has meaning and context for the learner and time must be given following the feedback for actions to be complete. Feedback on formative assessment must be constructive and provide clear guidance and actions for improvement. All records should be available for auditing purposes as we may choose to check records of formative assessment as part of our ongoing quality assurance. Formative assessments will not contribute to the overall mark of the units.

2: Summative Assessment

Summative assessment is used to evaluate learner competence and progression at the end of a unit or component. Summative assessment should take place when the assessor deems that the learner is at a stage where competence can be demonstrated.

Learners should be made aware that summative assessment outcomes are subject to confirmation by the Internal Verifier and External Quality Assurer (EQA) and thus is provisional and can be overridden. Assessors should annotate on the learner work where the evidence supports their decisions against the assessment criteria. Learners will need to

be familiar with the assessment and grading criteria so that they can understand the quality of what is required.

Formative Assessment	Summative Assessment
used during the learning process	used at the end of the learning process
provides feedback on learning-in-process	evaluates achievement against learning outcomes and assessment criteria
dialogue-based, ungraded	graded pass / refer

Evidence of both formative and summative assessment MUST be made available at the time of external quality assurance – EQA.

Course Regulations

Course Requirements

All units will be assessed internally using a range of methods. Knowledge-based outcomes can be assessed using non-mandatory assessment tasks (provided in this specification for tutors' convenience). Skills-based outcomes must be achieved with reference to a real work environment and must include direct observation within the workplace.

Classification of Awards

This qualification is graded as pass/fail.

Decisions about the overall achievements of awards are made by QUALIFI through the application of the academic and relevant course regulations. It is based on the Average Percentage Mark (APM) or, at the discretion of QUALIFI, on the basis of learners' overall profile and performance subject to the minimum requirements.

Learner Voice

Learners can play an important part in improving the quality of this course through the feedback they give. In addition to the on-going discussion with the course team throughout the year, there is a range of mechanisms for learners to feed back about their experience of teaching and learning.

Complaints

QUALIFI recognises that there may be occasions when learners and centres have cause for complaint about the service received. When this happens, the complaints procedure is intended to provide an accessible, fair and straightforward system that ensures as an effective, prompt and appropriate response as possible.

For more information, please contact in the first instance or email: support@QUALIFI-international.com

Unit Specifications

Unit CSEC01: Cyber Security Threat and Risk

Unit code: T/617/1129

RQF Level: 4

Unit Aim

Cyber security breaches cause significant personal and organisational damage and pose a clear and present risk to business profitability and resilience. Forbes, the business magazine, estimates that the annual cost of cyber-crime might reach (or surpass) $2Trillion by 2019. At a ground-level, Cyber security breaches are causing business insolvencies and posing challenges to employee safety and wellbeing.

In this unit the learner will be introduced to a variety of threats and risks emanating from the cyberspace. The unit will look at various methods of attack and will use case studies to analyse various threat vectors, including Malware, Botnets and Trojans.

The unit will introduce and explain various models of measuring threats, risks and impacts. Including, those proposed and recommended by a range of information security standards published by the International Standards Organisation and US NIST (National Institute of Standards and Technology). Using a well-documented 'real-world case study', the learner will investigate and examine the business impact of a recent mega data breach.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand complex business cyber security threats and risks.	1.1 Analyse major cyber breaches and methods of attack that have severely impacted businesses and public organisations. 1.2 Examine how to calculate the business impact of a suspected or actual cyber security breach.
2 Understand recent mega breaches and explain malware and ransomware attacks.	2.1 Apply threat and risk management concepts and models. 2.2 Explain the terms malware, ransomware and other forms of intentional malicious cyber attacks.

3	Understand how threats and malicious hackers are advancing and developing customised intrusion tools.	3.1	Discuss the development of customised intrusion tools and their use by malicious hackers.
		3.2	Analyse how an intrusion occurred to cause a mega data breach.

Indicative Content

- What are 'threat' and 'risk' in a computer security environment?
- Cyber security, current attack trends, methods and terminology
- Case studies in 'mega breaches', malware and ransomware attacks: what can we learn?
- Security and risk assessment: models and how to conduct analysis, including those recommended by ISO and NIST
- Cyber Threat Intelligence: Directing, Analysing, Disseminating, Action-On
- Business Impact Analysis

Suggested Resources

Bingley, R. (2015) *The Security Consultant's Handbook*, Ely: IT Governance Press

Krebs on Security (Online) accessed at: **https://krebsonsecurity.com/**

Palo Alto Networks (2016) *Cyber Security for Dummies* (2nd. Ed.) (New Jersey: John Wiley & Sons 2016)

Unit CSEC02: Network Security and Data Communications

Unit code: K/617/1130

RQF level: 4

Unit Aim

In this unit the learner will look at the component parts of digital communications and interoperability with IT networks, hardware, firmware and software components. The inherent insecurity of the internet will be described and discussed. What are the basics of computer science and technology? How do computers communicate with one another? How can networks communicate and how can we plan their security architecture in a more proactive and organised manner?

The second half of this unit will look at security planning and core concepts including 'security engineering', systems hardening and cyber resilience.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand how computers and digital devices communicate with one another over a network.	1.1 Analyse the core vulnerabilities within a network environment and an online environment. 1.2 Explain how the emergence of security thinking and tools can benefit a network environment.
2 Understand, at a strategic level how computer networking, web applications and software can be exploited.	2.1 Evaluate the link between network architecture and security engineering concepts.
3 Understand methods of security prevention and systems hardening.	3.1 Evaluate internal risks and exposure. 3.2 Evaluate available process and physical defences against malicious network intrusions.

4	Understand key network security and systems resilience tools, terminology and models.	4.1 4.2	Explain how key security concepts can be applied in a large and distributed organisation. Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience.

Indicative Content

- Network principles and protocols, security and systems resilience tools
- Security Engineering: Access controls, the CIA triad, systems hardening
- Software development and how it relates to cyber security risks
- Web applications and how they relate to risk
- Other key methods of malicious network attack
- Preventing and mitigating network attacks
- Cyber Resilience: Change Management and Configuration Management

Suggested Resources

Schneier on Security and the 'CryptoGram' newsletter accessed at: https://www.schneier.com/

Sikorski, M and Honig, A., (2012) *Practical Malware Analysis* (No Starch Press)

Solomon, M. G. Kim, D and Carrell, J. L. *Fundamentals of Communications and Networking* (Jones & Bartlett, 2014)

Unit CSEC03: Database Security and Computer Programming

Unit code: M/617/1131

RQF level: 4

Unit Aim

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. *Database security* is a specialist topic within the broader realms of computer security, information security and risk management.

In this unit the learner will explore security risks to database systems and mitigation techniques. Understanding the function of computer programming is essential to understanding the dark arts of 'Black Hat Hackers'. Learners will examine (as a rolling case study) Python as a popular contemporary programming language. The symbiotic link between developments in computer programming and vulnerabilities to hacking will be examined and explored.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand the broad range of information security controls to protect databases.	1.1 Explain security risks in database systems. 1.2 Assess the effectiveness of information security concepts and tools in protecting databases.
2 Understand types of database categories of control.	2.1 Explain database terminology and categories of control.
3 Understand the underpinning concepts and models of cloud-based storage solutions.	3.1 Explore the functionality of database tools available to Data Owners, Custodians, Incident Responders and Investigators.
4 Understand the relationship between computer programming	4.1 Explain various popular computer programming languages. 4.2 Analyse the relationship between programming

	and computer hacking.		skills and the ability to hack into systems.
5	Understand the 'interpreted' general-purpose programming language, Python.	5.1	Investigate where non-malicious and malicious hackers have utilised Python.

Indicative Content

- Database security breach types
- How various types of databases organise data, including the Grandfather-Father-Son model of Disaster Recovery
- Categories of control and the Anderson Rule
- Case studies in big data organisation and breach incidents
- Impact and utility of Cloud-based approaches
- Differences between compiled and interpreted programming languages
- Symbiotic relationship between developments in computer programming skills and hacking
- Introduction to understanding a popular programming language (Python)

Suggested Resources

Alfred Basta & Melissa Zgola (2011) *Database Security*, Boston: USA: Cengage Learning

Oracle Database Security Guide, accessed at:
https://docs.oracle.com/cd/E11882_01/network.112/e36292/toc.htm

Mark Lutz (2013) *Learning Python* (5th Ed.) Newton: USA, O'Reilly Media

Unit CSEC04: Incident Response, Investigations and Forensics

Unit code: T/617/1132

RQF level: 4

Aim

In this unit the learner will examine Incident Response, Computer Emergency Response Teams (CERTS), and events requiring investigative techniques. Learners will identify and examine aligned business tasks and task forces including Disaster Recovery, Business Continuity Management and Crisis Management.

The unit then focuses on exploring cyber-related incident investigations, including evidential analysis gathering, logging and reporting. Learners will have the opportunity to look at case studies and assess how the approaches used could be applied into their own workplace.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand the role and composite parts of Incident Response as a business function and how CERTS operate.	1.1 Explain the people, structures, processes and tools involved in Computer Incident Responses. 1.2 Discuss the different roles within a Computer Emergency Response Team and their importance.
2 Understand aligned task/task forces for Business Continuity, Disaster Recovery and Crisis Management.	2.1 Explain the terms BC, DR and CM. 2.2 Analyse the standards, protocols and concepts underpinning BC, DR and CR and their application within organisations.
3 Understand how major computer incidents are formally investigated.	3.1 Explain the processes, people and tools used in a planned and structured major incident investigation. 3.2 Analyse how evidence is contained, analysed, processed and deployed in a major cyber-related investigation.
4 Understand laws and guidance in relation to the	4.1 Examine how relevant laws and professional practice are applied to computer incident

conduct of planned and structured major incident investigations.	investigations.

Indicative Content

- CERTS: how to build the right teams to respond
- Incident Response: structure, people, scope
- Reporting and recording IR activity
- Aligned disciplines: Business Continuity Management, Disaster Recovery and Crisis Management
- Legal and ethical principles and computer network investigations
- Principles of forensic science and digital forensics
- Evidence handling: concepts, protocols and tools

Suggested Resources

Kawakami, J., (2016) Backups: Avoiding computer disasters on Windows, Mac and Linux, John Kawakami Publishing

'Krebs on Security' cyber security and news blog accessed at: **https://krebsonsecurity.com/**

Luttgens T., Pepe., M. and Mandia, K., (2014) *Incident Response & Computer* Forensics (3rd Ed.), McGraw Hill Education

Unit CSEC05: Security Strategy: Laws, Policies and Implementation

Unit code: A/617/1133

RQF level: 4

Unit Aim

Knowing how to build a cyber defence strategy, what legal tools require consideration, how policies can be written and embedded, are all vital ingredients to successful in-house cyber security practices.

In this unit the learner will bring together knowledge acquired from previous units and build on this in relation to developing plausible strategic plans, executive buy-in and legal compliance. Key questions and challenges are posed:

- What is 'strategy' and what can a 'cyber security strategy' look like?
- How do we achieve senior-level buy-in?
- How do we monitor and safeguard compliance, particularly if our operations are dispersed across a multinational environment?
- What are the key legal requirements and industry standards that can assist and enhance our cyber security strategies and practices?

Learning and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand the concept of strategy, strategic management, planning and buy-in in relation to cyber security.	1.1 Assess the value of strategic management and planning as applied to information security and cyber-enabled business environments.
2 Understand how legislation, formal industry standards, training and accreditations support cyber security.	2.1 Evaluate key legislation and industry standards that impact and assist cyber security planning. 2.2 Assess the key training and accreditation schemes relating to cyber security.
3 Understand how to implement Plan, Do, Check	3.1 Assess how to design, monitor, implement and continuously improve policies in relation to cyber

	and Act security and risk management policies.	and information risk business environments.
4	Understand the future legal and technical environment and the impact on cyber security planning and digital risk management.	4.1 Investigate the approaches of large influential countries in the information security domain. 4.2 Discuss relevant national/international regulatory and standards relating to cyber security environments.
5	Understand how to plan and design a security audit for a cyber network.	5.1 Design security plans that reflect the legal and political environment.

Indicative Content

- Strategic management, and how it applies to cyber security environments
- Cyber security policies and planning
- Legal, regulatory and standards bodies
- Training and further development – standards and training
- Future legal and technical environment and a range of national and international approaches
- Design a security audit

Suggested Resources

ISO (2013) ISO27001:2013 *Information Security Management*, International Standards Organisation (ISO)

NIST (Version 1, 2014) or (Version 1.1, 2018) : Cyber Security Framework (NIST CSF): Overview available at: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

Touhill, G, and Touhill, T.J (2014) *Cyber Security for Executives*, New York: Wiley

Unit 4IT06: Physical IT Networking

Unit code: K/617/6697

RQF Level: 4

Unit Aim

This unit aims to provide learners with knowledge of physical networking and basic network administration skills. It covers knowledge of computer networks.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Apply the components of physical networking.	1.1 Analyse the nature and requirements of a physical network. 1.2 Analyse the requirements of different networking standards. 1.3 Set up and configure LAN network devices to the required configuration.
2. Understand the components and interfaces between different physical networking attributes.	2.1 Analyse the requirements for the on-going maintenance of a physical network operating system. 2.2 Assess the implications of different connectivity considerations. 2.3 Analyse the purpose and implications of different protocols of the application layer.
3. Install security protocols in a physical network.	3.1 Install and configure a firewall to the required standard. 3.2 Document actions taken in response to threats to security to the required standard. 3.3 Determine the source and nature of threats to a network. 3.4 Take action to mitigate identified risks that is appropriate to the nature and scale of the risk.

Indicative Content

- Cabling and hardware standards
- Configuring a network operating system
- Ethernet
- Application layer

Suggested Resources

Lowe D (2018), Networking All-in-One for Dummies 7th Edition, John Wiley & Sons, New Jersey

Cisco e-Learning portal (http://cisco.netacad.net).

McNab C (2016) Network Security Assessment: Know Your Network, 3rd Edition, O'REilly

Unit DSC01: Cryptography

Unit code: J/617/4634

RQF level: 5

Unit Aim

The process of encrypting and decrypting information forms the basis of much computer, device and network security. Cryptography is designed and used to protect the confidentiality, integrity and authenticity of information. From the very beginnings of computing, and throughout the industry's evolution, the establishment of policies, guidelines and laws has shaped the disciplines of information security and organisational resilience in profound and, often, unintended, ways.

In this unit learners will be introduced to the concept and history of cryptography, and its subdisciplines (including cryptology), and how cyber-enabled networks and devices have their communications security underpinned by cryptographic methods and sector standards. Learners will explore methods of attack, including side-channel, additional encryption methods and escrow principles and key.

Learners will look at how businesses can deploy encryption to enhance their information security approaches.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand key cryptographic principles and modes.	1.1 Define the concept and application of cryptography. 1.2 Explain symmetric and asymmetric modes and approaches. 1.3 Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices .

2 Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption.	2.1 Explain the key principles of the related standards, regulations and laws and why they are in place. 2.2 Assess the consequences for organisations and individuals of non-compliance with these standards, regulations and laws.
3 Design an encryption plan and courses of action for a given organisation.	3.1 Explain the methods of attack used to target encrypted data. 3.2 Assess the additional encryption methods available. 3.3 Explain the key principles of escrow and recovery. 3.4 Explain the importance of having robust encryption arrangements within IT systems. 3.5 Evaluate the existing encryption arrangements. 3.6 Design an encryption plan to meet the needs of a given organisation, with recommended courses of actions.

Indicative Content

- The science of crypto
- Cipher types
- Symmetric and asymmetric
- Methods of attack
- Standards, regulations, legal domains
- Key escrow and recovery

Suggested Resources

Gordon Corera (2015) Intercept: The Secret History of Computers and Spies (London: W&N), available at: **https://www.amazon.co.uk/Intercept-Secret-History-Computers-Spies/dp/0297871730**

Krebs on Security (Online) accessed at: **https://krebsonsecurity.com/**

Lawrence Miller and Peter Gregory (2018) CISSP For Dummies (USA: John Wiley & Sons), available at: https://www.amazon.co.uk/CISSP-Dummies-Computers-Lawrence-Miller/dp/0470537914

Twitter - @GlobalCAcademy

-@bruceschneier

Unit DCS02: Digital Investigations and Forensics

Unit code: L/617/4635

RQF level: 5

Unit Aim

This unit describes and explains how to conduct investigations with cyber-enabled equipment, including on public-internet-facing networks, or other network environments. Much evidence is lost or ruled inadmissible within courts and tribunal environments because it has been mishandled and corrupted (or could have been) by investigators, or those with a perceived chain of custody over the data. Moreover, in a planet of several billion cyber-enabled devices, but few qualified cyber investigators, it is now the case that many organisations have to manage part or all of a cyber incident investigation, because the national CERT or police/security agencies are otherwise prioritised.

In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1 Understand the core principles of digital investigations.	1.1 Explain the investigation lifecycle from initiation to conclusion. 1.2 Explain how a 'digital' domain investigation is organised and managed.
2 Apply the types of tool that support professional digital investigations at a strategic	2.1 Analyse the range of tools that assist digital investigations in different situations. 2.2 Select the appropriate tools to carry out a digital

level.	investigation for a given situation, justifying the selection.
3. Plan for an investigations and forensics teams.	3.1 Explain the types of skills required to undertake a variety of investigations and forensic-related work. 3.2 Explain dynamics of forming and integrating digital investigation teams and geographically distributed and dispersed investigations and teams. 3.3 Develop a plan for the formation of an investigation and forensics teams.
4. Understand the importance of safeguarding evidential integrity in digital investigations.	4.1 Explain how evidence can be retrieved from mobile devices and IoT devices. 4.2 Analyse how evidential integrity is safeguarded during digital investigations. 4.3 Assess how evidence is stored and presented within legal environments.

Indicative Content

- Requirement for digital investigations
- Understanding evidential data and prospects of recovery
- Mobile, portable and apps in DI
- Evidential integrity and chain of custody
- Processes and timelines
- Legal domains and cross examination
- Management and budgeting

Suggested Resources

Bilton, N. (2017) American Kingpin: The Epic Hunt for The Criminal Mastermind Behind the Silk Road (Portfolio)

Sachowski, j. (2018) *Digital Forensics and Investigations: People, Processes and Technologies* (CRC Press)

Sikorski, M and Honig, A., (2012) *Practical Malware Analysis* (No Starch Press)

Unit 5IT04: System Administration

Unit code: R/617/6743

RQF Level: 5

Unit Aims

This unit aims to provide the knowledge needed to administer a system in Linux and Windows. Topics covered include user and group management; file system management; task automation; shell scripting; Dynamic Host Configuration Protocol (DHCP) servers; mail servers; domain name servers; files and printers sharing; basic utilities and tools; application management; registry; local and group policies; backup policies; restore policies and performance tuning.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Understand system administration.	1.1 Analyse the role of the system administrator. 1.2 Analyse the elements within system administration. 1.3 Analyse the history of the active directory and Lightweight Directory Access Protocol (LDAP). 1.4 Analyse the difference between snapshots and backups. 1.5 Analyse the differences between local and group policies on Windows and Linux 1.6 Analyse the role and requirements of backup and restore policies. 1.7 Analyse the requirements of managing applications.
2. Perform user management and file system management.	2.1 Write shell scripts that enable administration tasks to be performed on Linux and Windows systems: Get Help; Check Services; List Users and ping a list of servers. 2.2 Set up and configure users and groups

	to the agreed standard. 2.3 Install and configure file and printer sharing to agreed standards. 2.4 Write shell scripts to perform snapshots on Linux and Windows servers to agreed standards. 2.5 Tune performance through the application of a range of utilities and tools to agreed standards.

Indicative Content

- System administrators: duties, related fields; professional certification
- Managing users and groups
- Managing file systems
- Automating tasks, processes and Daemon
- Shell scripting
- PowerShell
- NFS, NIS servers and WINS servers
- File and printer sharing
- Application management
- Customizing with Registry
- Local and group policies
- Backup and restore policies
- Performance tuning

Suggested Resources

Nemeth E, Snyder G, Hein TR, Whaley B, Mackin D (2017): UNIX and Linux System Administration Handbook (5th edition), Addison-Wesley Professional

Frisch A (2002) Essential System Administration: Tools and Techniques for Linux and Unix Administration, 3rd Edition, O'Reilly Media, Sebastopol, CA, USA

Nickel J (2019) Mastering Identity and Access Management with Microsoft Azure: Empower users by managing and protecting identities and data, 2nd Edition, Packt Publishing

Unit 5IT05: Network Routing and Switching

Unit code: Y/617/6744

RQF Level: 5

Unit Aims

This unit aims to deliver the knowledge needed to carry out switching and the knowledge and skills needed to carry out routing – how to set up and configure a router and switches to interconnect a multi area network. The unit covers computer networks routing and switching including Router Information Protocol (RIP); Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF).

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Understand switching.	1.1 Evaluate the considerations to be taken into account in the purchase of a switch. 1.2 Analyse switching techniques and protocols. 1.3 Analyse the features in managed switches. 1.4 Analyse the differences between circuit switching and packet switching.
2. Perform routing.	2.1 Evaluate the considerations to be taken into account in making static and inter-VLAN routing decisions. 2.2 Analyse routing techniques and protocols. 2.3 Evaluate the considerations to be taken into account in dynamic routing. 2.4 Evaluate the considerations to be taken into account in a single and multi-area OSPF. 2.5 Set up and configure a single area OSPF to agreed standards. 2.6 Configure a multi area OSPF to agreed standards. 2.7 Configure a multi area EIGRP to agreed standards.

Indicative Content

- Switched networks
- Switching concepts and configuration
- Routing
- Inter-VLAN routing
- Static routing
- Routing dynamically
- Frame relay
- Single area OSPF and multi area OSPF
- EIGRP configuration and troubleshooting
- Networking access control lists

Suggested Resources

Diaz L (2018): CCNA Routing and Switching 200-125 Certification Guide, Packt Publishing

Cisco Networking Academy (2016) Routing and Switching Essentials v6 Companion Guide, Cisco Press, Indianapolis, USA

Emspon S (2016) CCNA Routing and Switching Portable Command Guide (ICND1 100-105, ICND2 200-105 and CCNA 200-125)

Unit 5IT06: Network Design and Administration

Unit code: D/617/6745

RQF Level: 5

Unit Aim

This unit aims to provide the knowledge and skills needed to enable learners to design a network i.e. how to scale and connect different networks to form an effective inter-connecting network. It covers hierarchical network design; gathering network requirements; identifying network performance issues.

Learning Outcomes and Assessment Criteria

Learning Outcomes When awarded credit for this unit, a learner will:	**Assessment Criteria** Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Understand network design.	1.1 Analyse the requirements of users. 1.2 Analyse the different layers in hierarchical network design. 1.3 Analyse competing protocols in link aggregation.
2. Configure a local area network and a VLAN.	2.1 Set up and configure a VLAN to agreed standards. 2.2 Analyse the requirements of connectivity and scaling. 2.3 Analyse the types and methods used in Network Address Translation (NAT). 2.4 Configure remote connections on Linux and Windows systems to agreed standards.
3. Administer a network.	3.1 Diagnose and resolve faults in the system. 3.2 Configure a network backbone using link aggregation that demonstrates a speed increase. 3.3 Analyse the history of the spanning tree protocol and its role in network redundancy. 3.4 Analyse the role of a network administrator. 3.5 Evaluate the technologies and applications available for network administration.

Indicative Content

- Scaling networks including bandwidth, availability resilience, class of service, quality of service and price)
- LAN redundancy
- Link aggregation
- Wireless LANS
- Hierarchical network design
- Connecting to the WAN
- Point-to-point connection
- Securing site-to-site connectivity
- Monitoring and troubleshooting the network
- DHCP
- Network address translation for IPv4
- Network utilities and tools
- DHCP servers
- DNS servers
- Web servers
- Mail servers
- Proxy servers
- SSH servers
- Directory service
- AAA servers
- GUI-based configuration for Linux servers
- Network Attached Storage (NAS)
- Virtualization
- Cloud computing
- Network management and design

Suggested Resources

Thomatis M (2017): Network Design Cookbook: 2nd edition, lulu.com

Dauti B (2017) Windows Server 2016 Administration Fundamentals: Deploy, set up and deliver network services with Windows Server while preparing for the MTA 98-365 exam and pass it with ease, Packt Publishing

Piper B (2017) Learn Cisco Network Administration in a Month of Lunches, Manning Publications

Contact Details

Customer service number: +44 (0) 1158882323

Email: support@QUALIFI-international.com

Website: www.QUALIFI.net www.QUALIFI-international.com