Qualifi Level 7 Diploma in Cyber Security

Qualification Specification

January 2024

Contents

Contents 2
About QUALIFI 4
Why Choose QUALIFI Qualifications? 4
Employer Support for the Qualification Development 4
Equality and Diversity 4
Qualification Title and Accreditation Number 5
Qualification Aims and Learning Outcomes 5
Aims of the QUALIFI Level 7 Diploma in Cyber Security 5
Learning Outcomes of the QUALIFI Level 7 Diploma in Cyber Security 5
Delivering the Qualification 6
External Quality Assurance Arrangements 6
Learner Induction and Registration 6
Entry Criteria 7
Recognition of Prior Learning 7
Data Protection 7
Learner Voice 8
Professional Development and Training for Centres 8
Progression and Links to other QUALIFI Programmes 8
Qualification Structure and Requirements 8
Credits and Total Qualification Time (TQT) 8
Rules of Combination for QUALIFI Level 7 Diploma in Cyber Security 9
Achievement Requirements 9
Awarding Classification/Grading 9
Assessment Strategy and Methods 10
Unit Specifications 11
Unit DCS701: Fundamentals of Cyber Security Technology 11
Unit DCS702: Network, Infrastructure and Systems Security 13
Unit DCS703: Applications of Cyber Security 15
Unit DCS704: Security management and governance 17
Unit DCS705: Cryptography 19

Contact Details 21

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 with 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.

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 with the qualification has its own RQF code. The QAN for this qualification is as follows:

QUALIFI Level 7 Diploma in Cyber Security (610/3596/8)

Qualification Aims and Learning Outcomes

Aims of the QUALIFI Level 7 Diploma in Cyber Security

The aim of the QUALIFI Level 7 Diploma in Cyber Security is to offer learners an advanced knowledge of the industry by deepening their awareness of cyber threats, vulnerabilities, and security technologies.

The core objective of the Qualifi Level 7 Diploma in Cyber Security qualification is to equip learners with the underpinning knowledge, understanding and skills required for a career in the cyber security sector.

The QUALIFI Level 7 Diploma in Cyber Security aims to give learners the opportunity to:

1. Gain a recognised qualification from an internationally recognised Awarding Organisation.
2. Develop research and critical thinking abilities to carry out independent cyber security research.
3. Develop competence in security management (risk assessment, compliance, and governance)
4. Gain in-depth knowledge of network security, digital forensics, ethical hacking, and cloud security.
5. Develop an understanding of ethical and legal aspects relating to privacy, compliance, and the legal frameworks that regulate cyber operations.

Learning Outcomes of the QUALIFI Level 7 Diploma in Cyber Security

The overall learning outcomes of the qualification are for learners to:

1. Recognise and analyse sophisticated cyber threats.
2. Create strong security architectures for enterprises, taking into account elements such as network security, data protection, and compliance with industry norms and regulations.
3. Establish and implement comprehensive security rules and procedures that are in line with a company's risk management plan
4. Understand the fundamentals of secure coding.
5. Conduct penetrating tests to examine an organisation's security posture and identify weaknesses.

6. Collaborate with cross-functional teams and communicate technical information to non-technical stakeholders.

The 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, 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.

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, 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 the learner's 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 the 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 20 or over.

Entry to the qualification will be through centre interviews and applicants will be expected to hold a Level 6 qualification. In certain circumstances learners who have relevant industry knowledge may be gain entry to the qualification.

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. The 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 support its approved centres with training related 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 7 Diploma in Cyber Security** will allow learners to progress to:

- A university partner, where they can complete a further 60 credits to receive a full master's degree
- Directly into employment in an associated profession.

Qualification Structure and Requirements

Credits and Total Qualification Time (TQT)

The QUALIFI Diploma in Cyber Security is made up of 120 credits which equates to 1200 hours 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 include 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 7 Diploma in Cyber Security

Learners are required to complete all four mandatory units plus four of the optional specialty units.

Unit Reference	Mandatory Units	Level	TQT	Credits	GLH
H/650/9532	Fundamentals of Cyber Security	7	200	20	100
J/650/9533	Network, Infrastructure and Systems Security	7	200	20	100
K/650/9534	Applications of Cyber Security	7	200	20	100
L/650/9535	Security Management and Governance	7	300	30	150
J/617/4634	Cryptography	7	300	30	150
		Total	**1200**	**120**	**600**

Achievement Requirements

Learners must demonstrate they have met all assessment criteria for all 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

This qualification is vocational and can support a learner's career progression. To meet QUALIFI's aim to provide an appropriate assessment method, each unit will be assessed through realistic 'real life' case study related written tasks. Learners will need to demonstrate knowledge and understanding of the academic material from the Unit, along with original creative thought and problem solving, plus they will need to provide recommendations based on the assignment and case scenario. Intellectual rigour will be expected that is appropriate to the level of the qualification.

The assignment tasks will address Learning Outcome and Assessment Criteria requirements, all of which must be demonstrated/passed in order to achieve the qualification. These 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.

The assessment tasks will require learners to draw on real life scenarios and 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 individuals and, wherever possible, encourage learners to draw on work-place opportunities to undertake research and investigation to support their learning.

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

Please contact Qualifi for further information.

Unit Specifications

Unit DCS701: Fundamentals of Cyber Security Technology

Unit code: H/650/9532
RQF level: 7

Unit Aim

The aim of this unit is to give learners an understanding if the key concepts of cyber security, allowing them to recognise and analyse security threats in a range of scenarios.

Learning Outcomes and Assessment Criteria

Learning Outcomes. When awarded credit for thisunit, a learner will:	Assessment Criteria. Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Understand the key concepts in cyber security.	1.1 Discuss what is meant by cyber security and its importance.
	1.2 Analyse the principal techniques and technologies used to achieve cyber security and the challenges faced.
2. Understand the impact of cyber security threats and attacks on individuals and organisations.	2.1 Analyse existing and emerging threats and the impact on individuals and organisations.
	2.2 Discuss the organisational policies and procedures that need to be in place to protect against cyber security attacks.
	2.3 Analyse how organisations can stay up to date with shifting cyber security threats and protect their operations and data.

Indicative Content

- SMART Objectives
- Cyber security threats, risks and vulnerabilities, threat landscape and attack vectors
- System vulnerabilities
- Legal responsibilities
- Physical security measures
- Software and hardware
- security measures Various Obstacles
- Delivery formats
- Network types
- Network components
- Networking infrastructure services and resources
- Importance of training staff on cyber security

Suggested Resources

Fundamentals of Cybersecurity [The Basics Guide]. (n.d.). https://www.knowledgehut.com/blog/security/cyber-security-fundamentals

Shea, S., Gillis, A. S., & Clark, C. (2023, January 11). What is cybersecurity? Security. https://www.techtarget.com/searchsecurity/definition/cybersecurity).

Unit DCS702: Network, Infrastructure and Systems Security

Unit code: J/650/9533
RQF level: 7

Unit Aim

The main objective of this unit is to for learners to gain an understanding of the various types of threats and vulnerabilities that can affect computer networks, infrastructure and systems, such as malware, hacking, and social engineering. It also aims to familiarise learners with various security technologies and tools, such as firewalls, intrusion detection systems, and encryption methods.

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 theycan:
1. Understand the security implications of networked systems.	1.1 Discuss the concepts and the role of • Network types • Network components • Networking infrastructure services and resources.
	1.2 Analyse network security protection methods
2. Understand the design and security of an organisational network.	2.1 Analyse operational technologies, the internet and critical infrastructure.
	2.2 Evaluate vulnerabilities and exploits that target computer networks and systems, the internet infrastructure.
	2.3 Assess approaches to modelling, assessing and testing networks and systems.
	2.4 Review access controls on a cyber-security network system and make recommendations as appropriate.

3 Understand networking topologies and how to secure them.	3.1 Explore that the different elements that affect network performance.
	3.2 Analyse present and future cyber security and information security technologies.
	3.3 Evaluate the strengths and weaknesses of a network for a given organisation in relation to cyber security.
4 Understand computer systems from the operating systems and security services.	4.1 Evaluate a range of deployments that support the worldwide web and distributed computing services.

Indicative Content

- Research methodologies
- Networking principles
- Firewalls, VPN, and Firmware
- Access logs
- Baselines and assurance
- Firmware updates
- End user device security
- Malware and Anti-virus protection
- Identify security weaknesses and focus on them
- End-point protection
- Security designs and related principles
- Internet and cloud computing/infrastructure

Suggested Resources

What is Network Security? The Different Types of Protections. Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

Network and System Security. (n.d.). ScienceDirect. https://www.sciencedirect.com/book/9780124166899/network-and-system-security

Network Security. (2023, March 21). GeeksforGeeks. https://www.geeksforgeeks.org/network-security/

Unit DCS703: Applications of Cyber Security

Unit code: K/650/9534
RQF level: 7

Unit Aim

The aim of this unit is to for learners to learn about the security measures and defence mechanisms that are used to defend against and respond effectively to security incidents, breaches, and anomalies.

Learning Outcomes and Assessment Criteria

Learning Outcomes. When awarded credit for this unit, a learnerwill:	**Assessment Criteria.** Assessment of this learning outcome will require a learner to demonstrate that they can:
1. Understand the principles around software and applications.	1.1 Analyse the issues of malicious software and the effect on the security of systems.
	1.2 Evaluate physical and infrastructure security measures to defend against attacks and threats.
	1.3 Explore defence mechanisms, host and application security.
2. Understand the techniques used for secure software development.	2.1 Discuss principles of secure programming.
	2.2 Explain common software vulnerabilities that can be introduced during software development.
	2.3 Analyse aspects of mobile and cloud security.
	2.4 Explore wider considerations and research directions for software and application security.

Indicative Content

- Limit the damage
- Disruption of attacks
- Restore operations
- Facing a cyber-security breach demands swift
- Strategic action to safeguard your assets, operations, and reputation
- Total costs
- Network trafficking
- Operating systems
- Incident resolution
- Task creation and management
- Human factors when securing networks and applications

Suggested Resources

Incident Response | Cyber Security Incident Response Services. (2023, October 9). Redscan. https://www.redscan.com/services/cyber-incident-response/

Wall, P. (2023, October 17). Define Your Incident Response Lifecycle | Application Security | Imperva. Learning Center. https://www.imperva.com/learn/application-security/define-security-incident-response/

Beaver, K. (2023, February 23). Top incident response tools: How to choose and use them. Security. https://www.techtarget.com/searchsecurity/feature/Incident-response-tools-How-when-and-why-to-use-them

Unit DCS704: Security management and governance

Unit code: L/650/9535
RQF level: 7

Unit Aim

The aim of this unit is to develop learners understanding of what constitutes effective security management in relation to different types of cyber threat that can affect organisations and individuals. Learners will have the opportunity to analyse and review a response to a cyber security incident.

Learning Outcomes and Assessment Criteria

Learning Outcomes. When awarded credit for this unit, a learnerwill:	**Assessment Criteria.** Assessment of this learning outcome will require a learner to demonstrate that theycan:
1. Understand the need for effective security management.	1.1 Critically review the main currently used approaches to management, including key standardised approaches and the fundamental importance of a risk-based approach.
2. Understand key components of practical cyber security management.	2.1 Discuss key related legislation and regulations and the impact on security management and importance for organisations to continuously monitoring their compliance.
	2.2 Analsye the importance of auditing in a security management context.
	2.3 Assess key role of people in achieving robust cyber security.
	2.4 Develop strategies to integrate a range of possible information security technologies and techniques into a security management system for a given organisation.
3. Understand how to respond to a cyber security incident effectively and the appropriate chain of events.	3.1 Explain the reporting processes involved in responding to a cyber security incident.
	3.2 Discuss the documentation that needs to be produced and maintained during and after a cyber security incident, including future actions.

	3.3 Analyse how to ensure business continuity during a cyber security incident.

Indicative content

- Data breaches
- Malware
- Cyber threats
- Attach vectors
- Zero-day vulnerabilities
- SQL injections
- Network infrastructure
- Emerging threats
- Legal compliance
- Data reports
- Data protection
- Record keeping
- Key standardised approaches and the fundamental importance of a risk-based approach

Suggested Resources

Cyber Security Threats and Countermeasures. Social Science Research Network; RELX Group (Netherlands). https://doi.org/10.2139/ssrn.4425678

Security Threats and Countermeasures | Global | Ricoh. (n.d.). Copyright RICOH Co., Ltd. https://www.ricoh.com/products/security/mfp/countermeasur.

Unit DCS705: Cryptography

Unit code: J/617/4634
RQF level: 7

Unit Aim

The aim of this unit is for learners to develop their understanding of cryptography, the different cryptography tools and how and when these tools are used.

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 theycan:
1. Understand the key concepts of cryptography and its limitations.	1.1 Analyse how the security of everyday digital applications tools is achieved and maintained.
	1.2 Explain the concepts of confidentiality and data integrity.
	1.3 Analyse the wider infrastructure surrounding cryptography and how this impacts the overall security of systems deploying cryptography.
2. Understand the function and purpose of the main cryptographic tools.	Explain how the main cryptographic tools are used. Assess the decision-making process used to select the most appropriate cryptographic tools to deploy in specific settings.

Indicative Content

- Backup and Restore
- Disaster Recovery
- Data Backup Solutions
- Data Replication and Data Restoration
- Backup Strategy
- Point-in-Time Recovery
- Data Loss Prevention
- Risk Tolerance
- Business Impact Analysis
- Security Risk Assessment
- Cyber-security Risk Management
- Risk Mitigation Strategies
- Risk Management Policies
- Risk Management Frameworks in Cyber-security

Suggested Resources

Data Backup & Recovery | Certitude Security | Cyber Security. (2023, February 10). Certitude Security. https://www.certitudesecurity.com/services/data-backup-and-recovery/

Cybersecurity Risk Management | Frameworks, Analysis & Assessment | Imperva. Learning Center. https://www.imperva.com/learn/data-security/cybersecurity-risk-management/

What is Cybersecurity Risk Management? Preventing Cyber Attacks | Up Guard. (n.d.). https://www.upguard.com/blog/cybersecurity-risk-management

Contact Details

Customer service number: +44 (0) 1158882323

Email: support@QUALIFI-international.com

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