Level 4 Certificate in Cyber Security Introduction (3660-01)

September 2019 Version 1.0

Qualification Handbook

Qualification at a glance

Subject area	IT Professional
City & Guilds number	3660-01
Age group approved	16+
Entry requirements	Centres must ensure that any pre-requisites stated in this Handbook are met.
Assessment	Online multiple choice test
Qualification grade scale	Pass
Approvals	Approval application required. Please see **www.cityandguilds.com** for details.
Registration and certification	Registration and certification of this qualification is through the Walled Garden, and is subject to end dates.

Title and level	GLH	TQT	City & Guilds qualification number	Ofqual accreditation number
Level 4 Certificate in Cyber Security Introduction	73	180	3660-01	TBC

Version and date	Change detail	Section
1.0 September 2019	Document created	

Contents

1 Introduction

This document tells you what you need to do to deliver the qualifications:

Area	Description
Who is the qualification for?	This qualification is designed to support learners to develop the underpinning knowledge that can be used as they progress in their chosen Cyber Security Apprenticeship specialism – either the 'Technologist' or 'Risk Assessment' pathways. This qualification forms the core knowledge module of the Level 4 Cyber Security Technologist apprenticeship that all apprentices will complete as a starting point, regardless of their chosen cyber security pathway. It is the foundation on which apprentices will build as they progress through their apprenticeship.
What does the qualification cover?	The aim of this qualification is to provide the learner with a broad introduction into what cyber security actually is, its building blocks and why it is important for organisations and wider society. It is designed to cover 'the essentials' of cyber security, introducing learners to the key concepts, terminology and processes that will support the learner when they move onto other qualifications in their chosen pathway, where they will explore these in more depth. The learner will explore the significant types of threats to information security, the techniques behind these attacks and the motivations of those responsible for attacks. They will then review the ways to defend against attacks and the processes organisations work through to manage the risk of attack. They will be familiar with the techniques that help in responding to a variety of evolving threats. Finally, they will review the legislation, standards and regulations that provide a framework within which cyber and information security is governed. This unit is a core part of the apprenticeship and forms part of both the Technologist and Risk Analyst pathways.

	Learners who complete this qualification will have the essential understanding required when they move into most cyber security roles.
What opportunities for progression are there?	On achieving this qualification the learner will have completed a section of the knowledge element as part of their apprenticeship journey either on the **Technologist** or **Risk Analyst** pathways: **Technologist pathway** • Level 4 Certificate in Cyber Security Introduction (3660-01) • Level 4 Certificate in Network and Digital Communications Theory (3660-02) • Level 4 Award in Security Case Development and Design Good Practice (3660-03) • Level 4 Award in Security Technology Building Blocks (3660-04) • Level 4 Certificate in Employment of Cryptography (3660-05) **Risk Analyst pathway** • Level 4 Certificate in Cyber Security Introduction (3660-01) • Level 4 Award in Risk Assessment in Cyber Security (3660-06) • Level 4 Certificate in Governance, Law, Regulation and Standards in Cyber Security (3660-07)
Who did we develop the qualification with?	It was developed in collaboration with employers, sector experts and training providers using the Apprenticeship Standard and Occupational Brief as the baseline. These were created by The Tech Partnership and their Employer Groups for the specific areas. The qualification embodies the required learning for an apprentice to have the opportunity to successfully gain the relevant knowledge for their chosen career path in cyber security.
Is it part of an apprenticeship framework or initiative?	Yes – Level 4 Cyber Security Technologist (9660-12/13)

Structure

Learners must complete the single unit 401 to gain this qualification.

Total Qualification Time

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

TQT is comprised of the following two elements:

- The number of hours which an awarding organisation has assigned to a qualification for Guided Learning, and
- An estimate of the number of hours a learner will reasonably be likely to spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by - but, unlike Guided Learning, not under the immediate guidance or supervision of - a lecturer, supervisor, tutor or other, appropriate provider of education or training

Title and level	GLH	TQT
Level 4 Certificate in Cyber Security Introduction	73	180

2 Centre requirements

Approval

To offer this qualification, new centres will need to gain both centre and qualification approval. Please refer to the *City & Guilds Centre Manual* for further information.

Centre staff should familiarise themselves with the structure, content and assessment requirements of the qualification before designing a course programme.

Resource requirements

Resources

Please see the individual unit information for any resources required.

Centre staffing

Staff delivering this qualification must be able to demonstrate that they meet the following occupational expertise requirements. They should:

- be occupationally competent or technically knowledgeable in the area[s] for which they are delivering training and/or have experience of providing training. This knowledge must be to the same level as the training being delivered
- have recent relevant experience in the specific area they will be assessing
- have credible experience of providing training

Centre staff may undertake more than one role, e.g. tutor and assessor or internal verifier, but cannot internally verify their own assessments.

Learner entry requirements

City & Guilds does not set entry requirements for this qualification. However, centres must ensure that candidates have the potential and opportunity to gain the qualification successfully and that they have the full engagement of the employer for the full programme.

Age restrictions

City & Guilds cannot accept any registrations for candidates under 16 as these qualifications are not approved for under 16s.

3 Delivering the qualification

Initial assessment and induction

An initial assessment of each candidate should be made before the start of their programme to identify:

- if the learner has any specific training needs
- support and guidance they may need when working towards their qualifications
- any units they have already completed, or credit they have accumulated which is relevant to the qualifications
- the appropriate type and level of qualification

We recommend that centres provide an induction programme so the candidate fully understands the requirements of the qualification, their responsibilities as a candidate, and the responsibilities of the centre. This information can be recorded on a learning contract.

Support materials

The following resources are available for this qualification:

- Practice exam available both paper-based and on-screen (the practice test contains 30 questions – pass mark is 23 out of 30)

4 Assessment

Summary of assessment methods

Candidates must:
- successfully complete one evolve test for the mandatory unit

Available assessments/assignments:

City & Guilds has written the following assessments to use with this qualification:

- Evolve tests

Assessment Types			
Unit	**Title**	**Assessment method**	**Where to obtain assessment materials**
401	Cyber Security Introduction	Multiple choice questions – online Evolve Test	Please see www.cityandguilds.com

Assessment strategy

Test specifications
The way the knowledge is covered by each test is laid out in the table below:

Assessment type: Multiple choice online test
Assessment conditions: Invigilated examination conditions
Number of questions: 35
Duration: 60 minutes
Pass mark: 26/35 (74%)
Grading: Pass/Fail

Test: 401 Cyber Security Introduction

Learning Outcome	Topic	Number of questions	Weighting
1 Understand cyber security theory	1.1 Confidentiality, Integrity and Availability	1	80%
	1.2 Management of hazards, threats, vulnerabilities and risks	6	
	1.3 Organisational Security	7	

	1.4 Attack vectors	8	
	1.5 Layered security	6	
2 Understand cyber security legislation, standards, regulations, and future trends	2.1 Cyber security legislation, standards, regulations	5	20%
	2.2 Threat landscape	2	
	2.3 Emerging trends		
Total		**35**	

Recognition of prior learning (RPL)

Recognition of prior learning means using a person's previous experience or qualifications which have already been achieved to contribute to a new qualification.

RPL is not allowed for this qualification.

5 Administration

Quality assurance

Internal quality assurance

Registered centres must have effective quality assurance systems to ensure optimum delivery and assessment of qualifications. Quality assurance includes initial centre registration by City & Guilds and the centre's own internal procedures for monitoring quality. Centres are responsible for internal quality assurance and City & Guilds is responsible for external quality assurance.

Standards and rigorous quality assurance are maintained by the use of:

- internal quality assurance
- City & Guilds external moderation

In order to carry out the quality assurance role, Internal Quality Assurers must have appropriate teaching and vocational knowledge and expertise.

Access arrangements and special consideration

We have taken note of the provisions of equalities legislation in developing and administering this specification.

We follow the guidelines in the Joint Council for Qualifications (JCQ) document: Regulations and Guidance Relating to Candidates who are Eligible for Adjustments in Examination GCSE, GCE, GNVQ, AEA, Entry Level, Basic Skills & Key Skills Access Arrangements and Special Consideration. This is published on the JCQ website: http://www.jcq.org.uk/access_arrangements/

Access arrangements

We can make arrangements so that learners with disabilities, special educational needs and temporary injuries can access the assessment. These arrangements must be made before the examination. For example, we can produce a Braille paper for a learner with visual impairment.

Special consideration

We can give special consideration to learners who have had a temporary illness, injury or indisposition at the time of the examination. Where we do this, it is given after the examination.

Applications for either access arrangements or special consideration should be submitted to City & Guilds by the Examinations Officer at the centre.

Language of examinations

We will provide this specification in English only.

Other issues

European Dimension

City & Guilds has taken account of the 1988 Resolution of the Council of the European Community in preparing this specification and associated specimen units.

Environmental Education

City & Guilds has taken account of the 1988 Resolution of the Council of the European Community and the Report Environmental Responsibility: An Agenda for Further and Higher Education 1993 in preparing this specification and associated specimen units.

Avoidance of bias

City & Guilds has taken great care in the preparation of this specification and specimen units to avoid bias of any kind.

6 Units

Availability of units

The unit information can be found in this document.

Structure of the units

These units each have the following:

- City & Guilds reference number
- Title
- Level
- Guided learning hours (GLH)
- Learning outcomes

Centres must deliver the full breadth of the range. Specialist equipment or commodities may not be available to all centres, so centres should ensure that their delivery covers their use.

Unit 401 Cyber Security Introduction

Level:	4 Certificate
GLH:	73
TQT:	180

What is this unit about?

The aim of this unit is to provide the learner with a broad introduction into what cyber security actually is, its building blocks and why it is important for organisations and wider society. It is designed to cover 'the essentials' of cyber security, introducing learners to the key concepts, terminology and processes that will support the learner when they move onto other units in their chosen pathway, where they will explore these in more depth.

The learner will explore the significant types of threats to information security, the techniques behind these attacks and the motivations of those responsible for attacks. They will then review the ways to defend against attacks and the processes organisations work through to manage the risk of attack. They will be familiar with the techniques that help in responding to a variety of evolving threats.

Finally, they will review the legislation, standards and regulations that provide a framework within which cyber and information security is governed.

This unit is a core part of the apprenticeship and forms part of both the Technologist and Risk Analyst pathways.

Learners who complete this unit will have the essential understanding required when they move into most cyber security roles.

This unit is assessed through a multiple-choice test, taken online.

Learning outcomes

In this unit, learners will be able to:

1. Understand cyber security theory
2. Understand cyber security legislation, standards, regulations, and future trends

Learning outcome

The learner will:

1. Understand cyber security theory

Topics

1.1 Confidentiality, Integrity and Availability (CIA)
1.2 Management of hazards, threats, vulnerabilities and risks
1.3 Organisational Security
1.4 Attack vectors
1.5 Layered security

Depth

Topic 1.1

The learner will be able to explain the elements of the CIA triad:

- Confidentiality:
  - Document classification
  - Privacy measures, data safeguarding
  - Encryption
- Integrity:
  - Hashing
  - Version control
  - Non-repudiation
- Availability:
  - System Upgrades
  - Bottlenecks
  - Redundancy
  - Scalability

Topic 1.2

The learner will be able to describe hazards, threats, and vulnerabilities and how each relate and lead to risk:

- Hazards:
  - Environmental, such as: flood, fire
- Threats:
  - Threat actors, such as:
    - Cyber criminals
    - Hacktivists
    - State-sponsored
    - Trusted Insider
  - Threat vector e.g. malware
- Vulnerabilities, such as:
  - Backdoors
  - Unpatched systems
  - Obsolescence
  - Software flaws

The learner will be able to describe the impact of a loss of CIA:

- Organisational, such as:
  - Damage to reputation
  - Legal costs
  - Regulatory sanctions
  - Loss of revenue
- Society and economy, such as:
  - Threat to economic stability and growth
  - Risks to critical national infrastructure (CNI)

    - Undermining of democratic processes, institutions and referendums
    - Creation of a market to sell cyber-crime skills and tools to non-experienced individuals

The learner will be able to describe how organisations develop their approach to risk management:

- Governance, linked to business strategy
- Identification, such as:
    - Threat intelligence
    - Threat profiling
    - Threat modelling
- Assessment
- Classification
- Reporting
- Assurance
- Management strategies:
    - Acceptance
    - Avoidance
    - Mitigation
    - Transfer
- Incident response and recovery
- Using recognised risk management frameworks, such as NIST SP 800 30 and ISO 27005

Topic 1.3

The learner will be able to explain how organisations secure information including describing the concepts of trusted and trustworthy, with respect to the following:

- Safety - the ability of the system to operate without harmful states
- Reliability - the ability of the system to deliver services as specified
- Availability - the ability of the system to deliver services when requested
- Resilience - the ability of the system to transform, renew and recover in a timely way in response to events
- Security - the ability of the system to remain protected against accidental or deliberate attack

The learner will be able to explain the benefits and limitations of different approaches to assurance:

- Intrinsic:
    - Software design, development and implementation
    - Segregated lab testing, such as sandbox, whitebox and blackbox
    - Control design and performance
    - Security baselines, such as benchmarking
    - Procedures and processes that validate security
- Extrinsic:
    - Security testing, such as vulnerability assessment, penetration testing and simulated attack exercises
    - Supply chain assurance

- Policies and procedures

Topic 1.4

The learner will be able to analyse the main types of attacks, attack techniques, how they work, why they are effective and how they continuously evolve:

- Social engineering, such as Phishing and Vishing
- Malware, such as Ransomware, Stegomalware, Steganography and Scareware
- Network interception
- Escalation of privileges
- Advanced Persistent Threat (APT)
- Denial of service (DoS) / Distributed Denial of Service (DDoS)

The learner will be able to explain the role of human behaviour in cyber security:

- Training, awareness and monitoring of cyber security practice (cyber culture)
- The insider threat:
  - Compromised employee, such as coercion, bribery
  - Disgruntled employees
  - Embedded contractors
  - Connected business partners
  - Human error
- The motives for cyber-crime:
  - Financial gain
  - Vindictive or disgruntled employees
  - Government-to-government crime
  - The challenge / peer group motivation
  - Supporting a cause

Topic 1.5

The learner will be able to explain layered security when deploying a system in an organisational context:

- Physical
- Network
  - Cloud
  - Virtualisation
- Application
- End point
- Data

Learning outcome

The learner will:

2. Understand cyber security legislation, standards, regulations, and future trends

Topics

2.1 Cyber security legislation, standards, regulations

2.2 Threat landscape

2.3 Emerging trends

Depth

Topic 2.1

The learner will be able to describe key legislation, standards, regulations, why they are important and the responsibilities they place on organisations and individuals. They will be able to explain the context in which they are used and the differences between them:

UK legislation:

- Computer Misuse Act
- Data Protection Act combined with the General Data Protection Regulation
- Human Rights Act
- Electronics Communications Act
- Official Secrets Act
- Regulation of Investigatory Powers Act (RIPA)
- Telecomms (Lawful Business Practice) (Interception of Communications) Regulation

International law:

- Digital Millennium Act

Organisational policies and processes, such as:

- Acceptable use (computer/internet)
- Access Control Policy
- Disclosure
- Data protection
- Security
- Disaster recovery
- Data retention
- Vulnerability management
- Privacy (informing staff they may be monitored (CCTV, email monitoring))
- Ethics
- Codes of conduct

Professional and Certification bodies:

- British Computer Society (BCS)
- Chartered Institute of information Security (CIIS)
- CISCO
- Cloud Security Alliance (CSA)
- CompTIA
- Council of Registered Ethical Security Testers (CREST)

- The Institution of Engineering and Technology (IET)
- ISACA
- ISC^2
- Microsoft
- Security Institute

Technical Standards and Frameworks, such as:

- Cloud Controls Matrix
- FIPS-140-2
- ISO270001/270002
- National Cyber Security Centre (NCSC), including Cyber Essentials, Cyber Essentials Plus
- PAS555
- PCI-DSS
- TOGAF

Topic 2.2

The learner will be able to describe and evaluate the sources of information about the current threat landscape:

- National Cyber Security Centre (NCSC)
    - Cyber Security Information Sharing Partnership (CiSP)
- Warning, Advice and Reporting Points (WARPS)
- Private threat intelligence companies

Topic 2.3

The learner will be able to describe and evaluate the sources of information for identifying emerging trends within cyber security:

- Horizon scanning
- Cyber security conferences
- Private companies
- Online research
- Market trend reports
- Professional journals
- Academic research papers
- Government sponsored sources, such as White Papers

Supporting Information

Guidance for delivery

This unit is the core unit that all apprentices will complete as a starting point, regardless of their chosen cyber security pathway. It is the foundation on which apprentices will build as they progress through their apprenticeship. The unit introduces them to the core concepts, terminology and processes they will encounter in the world of cyber security and which they will explore in greater depth in further units. Consequently, tutors should consider the relevant pathways their apprentices are on and the qualifications they will take to maximise learning opportunities and to embed the learning. For example, an apprentice completing the Risk Analyst pathway will also need to complete 3660-07 Governance, Law, Regulation and Standards so they will 'dive deeper' into the relevant areas that are introduced in this unit.

It is expected that tutors will want to 'bring to life' many of the concepts contained in this unit especially those relating to types of attack, typical attack techniques and the lessons that were learned from them. This will be an opportunity to discuss 'case studies' - real-world examples such as the NHS Denial of Service (DoS) attack of 2017 or other examples from the world of cyber security. Other examples of non-typical or unforeseen attacks can be introduced – for example, rolling out a new system without sufficient testing or checks which can create issues but which are not connected with a threat actor. There are also examples of natural hazards such as fire or flooding which can unintentionally but critically impact the world of information security – such as the fire in Buncefield in the United Kingdom 2005 which affected local buildings holding information systems https://en.wikipedia.org/wiki/Buncefield_fire

Suggested learning resources

Websites

The Institute of Engineering and Technology
https://www.theiet.org

Institute of Information Security Professionals
https://www.iisp.org/

Ethical Security Testers (CREST)
http://www.crest-approved.org/

The British Computer Society (BCS)
https://www.bcs.org

The Information Commissioners Office
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Information on the UK adoption of Network and Information Security Directive
https://www.twobirds.com/en/news/articles/2018/uk/uk-adoption-of-network-and-information-security-directive

7 Sources of general information

The following documents contain essential information for centres delivering City & Guilds qualifications. They should be referred to in conjunction with this handbook. To download the documents and to find other useful documents, go to the Centres and Training Providers homepage on www.cityandguilds.com.

Centre Manual - Supporting Customer Excellence contains detailed information about the processes which must be followed and requirements which must be met for a centre to achieve 'approved centre' status, or to offer a particular qualification, as well as updates and good practice exemplars for City & Guilds assessment and policy issues.

Specifically, the document includes sections on:

- The centre and qualification approval process
- Assessment, internal quality assurance and examination roles at the centre
- Registration and certification of candidates
- Non-compliance
- Complaints and appeals
- Equal opportunities
- Data protection
- Management systems
- Maintaining records
- Assessment
- Internal quality assurance
- External quality assurance.

Our Quality Assurance Requirements encompasses all of the relevant requirements of key regulatory documents such as:

- SQA Awarding Body Criteria (2007)
- NVQ Code of Practice (2006)

and sets out the criteria that centres should adhere to pre and post centre and qualification approval.

Access to Assessment & Qualifications provides full details of the arrangements that may be made to facilitate access to assessments and qualifications for candidates who are eligible for adjustments in assessment.

The **centre homepage** section of the City & Guilds website also contains useful information on such things as:

- **Walled Garden**: how to register and certificate candidates on line
- **Events:** dates and information on the latest Centre events
- **Online assessment**: how to register for e-assessments.

Centre Guide – Delivering International Qualifications contains detailed information about the processes which must be followed and requirements which must be met for a centre to achieve 'approved centre' status, or to offer a particular qualification.

Specifically, the document includes sections on:

- The centre and qualification approval process and forms
- Assessment, verification and examination roles at the centre
- Registration and certification of candidates
- Non-compliance
- Complaints and appeals
- Equal opportunities
- Data protection
- Frequently asked questions.

Linking to this document from web pages

We regularly update the name of documents on our website, therefore in order to prevent broken links we recommend that you link to our web page that the document resides upon, rather than linking to the document itself.

8 Useful contacts

UK learners General qualification information	**E: learnersupport@cityandguilds.com**
International learners General qualification information	**E: intcg@cityandguilds.com**
Centres Exam entries, Certificates, Registrations/enrolment, Invoices, Missing or late exam materials, Nominal roll reports, Results	**E: centresupport@cityandguilds.com**
Single subject qualifications Exam entries, Results, Certification, Missing or late exam materials, Incorrect exam papers, Forms request (BB, results entry), Exam date and time change	**E: singlesubjects@cityandguilds.com**
International awards Results, Entries, Enrolments, Invoices, Missing or late exam materials, Nominal roll reports	**E: intops@cityandguilds.com**
Walled Garden Re-issue of password or username, Technical problems, Entries, Results, e-assessment, Navigation, User/menu option, Problems	**E: walledgarden@cityandguilds.com**
Employer Employer solutions including, Employer Recognition: Endorsement, Accreditation and Quality Mark, Consultancy, Mapping and Specialist Training Delivery	**E: business@cityandguilds.com**

If you have a complaint, or any suggestions for improvement about any of the services that we provide, email: **feedbackandcomplaints@cityandguilds.com**

About City & Guilds

As the UK's leading vocational education organisation, City & Guilds is leading the talent revolution by inspiring people to unlock their potential and develop their skills. We offer over 500 qualifications across 28 industries through 8500 centres worldwide and award around two million certificates every year. City & Guilds is recognised and respected by employers across the world as a sign of quality and exceptional training.

City & Guilds Group

The City & Guilds Group is a leader in global skills development. Our purpose is to help people and organisations to develop their skills for personal and economic growth. Made up of City & Guilds, City & Guilds Kineo, The Oxford Group and ILM, we work with education providers, businesses and governments in over 100 countries.

Copyright

Published by City & Guilds, a registered charity established to promote education and training

City & Guilds
5-6 Giltspur House
London EC1A 9DE
www.cityandguilds.com