Level 4 Award in Security Technology Building Blocks (3660-04)

September 2019 Version 1.0

Qualification Handbook

Qualification at a glance

Subject area	IT Professional
City & Guilds number	3660
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 Award in Security Technology Building Blocks	46	111	3660-04	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 who are on the **Technologist** pathway of the **Level 4 Cyber Security Technologist** apprenticeship, forming a mandatory qualification in that pathway.
What does the qualification cover?	The purpose of this qualification is to provider learners with the knowledge required to identify and describe the hardware and software components used to secure a networked IT system, and the role those components perform in respect of securing the system.
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 on the **Technologist** pathway: **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)
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 404 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 Award in Security Technology Building Blocks	46	111

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

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**
404	Security Technology Building Blocks	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: 20
Duration: 30 minutes
Pass mark: 14/20 (70%)
Grading: Pass/Fail

Test: 404 Security Technology Building Blocks

Learning Outcome	Topic	Number of questions	Weighting
1 Describe the technology components that are involved in securing a networked IT system	1.1 Hardware components	5	65%

	1.2 Software components	3	
	1.3 Risk mitigation	5	
2 Explain the role technology components perform in securing a networked IT system	2.1 Design networked IT systems for security	2	35%
	2.2 Deploying network technology components to provide security functionality	5	
Total		**20**	

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 404 Security Technology Building Blocks

Level:	4 Award
GLH:	46
TQT:	111

What is this unit about?

The purpose of this unit is to provider learners with the knowledge required to identify and describe the hardware and software components used to secure a networked IT system, and the role those components perform in respect of securing the system.

This unit is a mandatory unit for apprentices completing the 'Technologist' pathway of the Level 4 Cyber Security Technologist apprenticeship.

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

Learning outcomes

In this unit, learners will be able to

1. Describe the technology components that are involved in securing a networked IT system
2. Explain the role technology components perform in securing a networked IT system

Learning outcome

1. Describe the technology components that are involved in securing a networked IT system

Topics

1.1 Hardware components
1.2 Software components
1.3 Risk mitigation

Depth

Topic 1.1

The learner will be able to describe the typical hardware components involved in securing networked IT systems:
Inside the network infrastructure, such as:

- Cabling and Network Interface:
    - Characteristics:
        - Speed
        - Attenuation
        - Segment length
        - Baseband/broadband
    - Copper:

        - Cat 3
        - Cat 5
        - Cat 5e
        - Cat 6
        - Cat 6a
        - Cat 7
        - Cat 8
        - Shielded Twittered Pair (STP)
    - Optical:
        - Single mode
        - Multi-mode
    - Wireless
    - Network adapters
- Repeaters
- Bridges
- Switches
- Hubs
- Routers:
    - Wired
    - Wireless
- Wireless Access Point (WAP)
- Network Address Translator
- Gateways / Modems
- Hardware Firewalls:
    - Stateful
    - Stateless
    - Next generation firewalls
- Circuit level gateways
- Intrusion detection systems (IDS):
    - Host based Intrusion Detection Systems (HIDS)
    - Network based Intrusion Detection Systems (NIDS)
- Intrusion prevention systems (IPS):
    - Host based Intrusion Protection Systems (HIPS)
    - Network based Intrusion Protection Systems (NIPS)

Outside the network infrastructure, such as:

- Hardware Security Modules (HSM):
    - Certification Authority modules
    - Card payment system modules
    - Cryptographic network adapters
    - Cryptowallets
    - Trusted Platform Modules (Cryptoprocessor)
- Physical and logical access controls to servers and network infrastructure:
    - Mantrap
    - Cypher locks
    - Electromagnetic bolts

    - Biometrics, such as:
        - Retinal scans
        - Fingerprint scanning
    - Security/ reception staff
    - Closed Circuit Television (CCTV)

Topic 1.2

The learner will be able to describe the typical software components involved in securing networked IT systems:

Software installed on systems, such as:

- Trusted Operating Systems
- Directory services:
    - LDAP
    - Active Directory
- Network Traffic monitors
- Application gateways
- Software Firewalls
- Intrusion detection systems (IDS):
    - Network Intrusion detection systems (NIDS)
    - Host Intrusion detection systems (HIDS)
- Intrusion prevention systems (IPS):
    - Host based Intrusion Protection Systems (HIPS)
    - Network based Intrusion Protection Systems (NIPS)
- Network management software:
    - Simple Network Management Protocol (SNMP):
        - Management Information Base (MIB)
        - SNMP manager
        - SMP Agent
        - SNMP managed devices and resources
    - Internet Message Control Protocol (ICMP)
- Anti-malware detection and prevention systems:
    - Honeypot
    - Anti-malware
    - Anti-virus
    - Anti-Spam
    - Pop up blockers
- Identity and access management software:
    - One-time passwords
- End-to-End Encryption software
- Web Analytics Tracking modules
- DNS Filtering
- Proxy Servers
- Machine Learning tools (Artificial Intelligence)
- Unified Threat Management tools (UTM)
- Security Information and Event Management (SIEM)

Network virtualization and segregation, such as:

- Network segregation (VLANs)
- Virtual Private Networks (VPNs)
- De-Militarised Zones (DMZ)

Topic 1.3

The learner will be able to describe the key aspects of risk mitigation and how, despite this, residual risks will typically remain and the approach to take with these. They will be able to analyse the assurance of key components that support good risk management:

- How each component is used to mitigate risk in a network:
    - Switches:
        - MAC address filtering
        - Access control lists (ACLs)
    - Routers:
        - ACLs
    - Firewalls:
        - Stateful
        - Stateless
    - IDS
    - IPS
    - Next generation firewalls
    - Redundant Array of Inexpensive Disks (RAID):
        - 0
        - 1
        - 5
        - 10
- The security benefits and drawbacks of each component considering the impact upon:
    - Performance
    - Capacity
    - Availability

The learner will be able to explain the residual risk inherent in any network component:

- Design flaws
- Backdoors, such as:
    - Trojans
- Malicious code, such as:
    - Viruses
    - Ransomware
- Component failure, such as:
    - CPU
    - RAM
    - PSU
    - BIOS/UEFI
    - Expansion cards
    - Fans

    - UPS batteries
- End of life systems
- Failsafe states:
    - Where the failsafe state introduces a vulnerability – such as physical security controls defaulting to the open access state in the event of a power failure
- False positives/negatives:
    - Environmental conditions
    - Invalid inputs

The learner will be able to explain the implicit assurance of components in a networked IT system:

- Supplier warranties
- Service Level Agreement (SLA)
- Memorandum of agreement (MOU)
- Independent testing / certification
- Key escrow
- Patching/upgrades
- Implications of open versus closed source

Learning outcome

2. Explain the role technology components perform in securing a networked IT system

Topics

2.1 Design networked IT systems for security

2.2 Deploying network technology components to provide security functionality

Depth

Topic 2.1

The learner will be able to describe how hardware and software components contribute to security in a network, such as:

- Redundancy:
    - High-availability clusters
    - Failover
    - DNS Lookup zones:
        - Primary
        - Secondary
        - Forward
        - Reverse
- Network segmentation
- Traffic filtering
- Application Management
- Remote access and management:
    - Remote Desktop Protocol (RDP)

- Data Encryption
- Access control:
  - Authentication
  - Authorisation
- Monitoring:
  - Intrusion detection
  - Intrusion prevention
- Auditing
- Security baselines
- Behavioural analytics

Topic 2.2

The learner will be able to explain:

- Use of components to create a secure IT system:
  - On-premise/enterprise:
    - System hardening
    - EMI shielding
    - RFI shielding
    - Fire suppression
    - Hot and Cold isles
  - Cloud:
    - Architectural Models:
      - Public
      - Private
      - Hybrid
      - Community
    - Delivery models:
      - Infrastructure as a Service (IaaS)
      - Platform as a Service (PaaS)
      - Software as a Service (SaaS)
  - Virtualization platforms:
    - Types of Hypervisors:
      - Type 1
      - Type 2
    - Types of Virtualisation:
      - Desktop
      - Hardware
      - Network
      - Storage
- Human factors in a secure IT system, such as:
  - Organizational Security culture management
  - Information Security Policy:
    - Governance / Standards:
      - ISO/IEC 22301 - Business continuity management systems (BCMSs)

            - ISO/IEC 27001 - International Standard for best-practice information security management systems (ISMSs)
            - ISO/IEC 27032 - International Standard focusing explicitly on cyber security
            - ISO/IEC 27035 - International Standard for incident management
            - US Assurance Standards:
                - SOC 1
                - SOC 2
            - IASME (Information Assurance for Small and Medium Enterprises) Governance Standard
            - Cloud Control Matrix (CCM)
            - Payment Card Industry Data Security Standard (PCI DSS)
        - Policies:
            - Acceptable usage
            - Data Retention
            - Acceptable Use
            - Access Control
            - Communication
        - Compliance monitoring:
            - Network security
            - Data security
    - Information Security Procedures:
        - Training
        - Documentation
        - Monitoring
- Access control, such as:
    - Directory Services
    - Mandatory Access Control (MAC)
    - Discretionary Access Control (DAC)
    - Role Based Access Control (RBAC)
    - Rule Based access Control
    - Multi factor authentication:
        - Usernames and passwords
        - Biometrics
        - Personal Identification Number (PIN)
        - One-time passwords
        - USB hardware token
- Monitoring of activity in networked IT systems, such as:
    - Network traffic:
        - Protocol analyser
        - Port scanner
    - User access
    - System failures
    - Activity logs:
        - System logs
        - Security logs
        - Events viewer

    - Intrusions:
        - IDS
        - Security logs
- Testing of networked IT hardware and software components, such as:
    - Penetration testing
    - Configuration testing
    - Load testing
    - Static code analysis
    - 'Red Teaming' – common attack exploits
    - Security functionality testing – software security functions

Supporting Information

Guidance for delivery

Delivery of this unit will benefit from following a network layering model as the basis for mapping the physical and logical components of network infrastructure and explaining their role in securing access to the network and the resources connected to the network – servers, storage, applications and data.

The unit should be constrained to those aspects of the network infrastructure that directly impact upon security, including the physical network components, software components and any direct access controls to the network (such as two factor authentication and MAC address filtering) that ensures only those persons and devices authorised may access the network and resources connected to it.

A unified use case scenario will be helpful for teaching the role of each component in the network, positioning its relationship to other components and describing how each component contributes to the overall security of the network.

Topic 1.3 - The banning of ZTEs products by the US government is a good example to highlight in this topic area, where even secure hardware can include code that is intended to do harm by design.

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