Get help and support
Visit our website for information, guidance, support and resources at aqa.org.uk/tech-levels
E: techlevels@aqa.org.uk
T: 0800 085 0391

LEVEL 3
FOUNDATION TECHNICAL LEVEL
IT: CYBER SECURITY
360 GLH (TVQ01010)

LEVEL 3
TECHNICAL LEVEL
IT: CYBER SECURITY AND SECURITY ADMINISTRATION
720 GLH (TVQ01009)

Specifications
First registration September 2015 onwards

Version 3.1 November 2018
## Contents

1 About these qualifications 7

2 Qualification at a glance – overview 8

   2.1 Level 3 Foundation Technical Level IT: Cyber Security 8
   2.2 Level 3 Technical Level IT: Cyber Security and Security Administration 10

3 Level 3 Foundation Technical Level IT: Cyber Security: Statement of purpose 12

   3.1 Qualification objectives 12
   3.2 Who is this qualification for? 12
   3.3 What does this qualification cover? 13
   3.4 What could this qualification lead to? 13
   3.5 Who supports this qualification? 14
   3.6 What are the benefits of this qualification? 16
   3.7 Links to professional body memberships 17

4 Level 3 Foundation Technical Level IT: Cyber Security: Unit summary 18

5 Level 3 Technical Level IT: Cyber Security and Security Administration: Statement of purpose 19

   5.1 Qualification objectives 19
   5.2 Who is this qualification for? 19
   5.3 What does this qualification cover? 20
   5.4 What could this qualification lead to? 21
   5.5 Who supports this qualification? 21
   5.6 What are the benefits of this qualification? 24
   5.7 Links to trailblazers 25
   5.8 Links to professional body memberships 25

6 Level 3 Technical Level IT: Cyber Security and Security Administration: Unit summary 26

7 Meaningful employer involvement 27

   7.1 Introduction 27
   7.2 Definition of meaningful employer involvement 27
   7.3 Employer involvement in quality assurance 28

8 Synoptic delivery and assessment 29

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
9 Total qualification time 31
10 Transferable skills 32
11 Support materials and guidance 34
12 Qualification units 35
  12.1 Unit 1: Fundamental principles of computing 35
  12.2 Unit 2: Communication technologies 46
  12.3 Unit 3: Developing and maintaining computer networks 56
  12.4 Unit 4: Network threats and vulnerabilities 71
  12.5 Unit 5: Maths for computing 90
  12.6 Unit 6: Network and cyber security administration 103
  12.7 Unit 7: Managing identity and access to systems 123
  12.8 Unit 8: Programming for networking and security (optional) 142
  12.9 Unit 9: Computer forensic investigation (optional) 161
13 Externally set and marked examinations 174
  13.1 Introduction 174
  13.2 Examination format and structure 175
  13.3 Reasonable adjustments and special considerations 175
  13.4 Availability of past examination papers 175
14 External quality assurance 176
  14.1 Overview 176
  14.2 Quality assurance visits 176
  14.3 Sanctions 177
15 Internal assessment and quality assurance 178
  15.1 Overview 178
  15.2 Role of the assessor 178
  15.3 Assessor qualifications and experience 179
  15.4 Applying portfolio assessment criteria 179
  15.5 Authentication of learner work 179
  15.6 Tutor assistance and feedback 179
  15.7 Research and references 180
  15.8 Role of the internal quality assurer 180
  15.9 Internal quality assurer qualifications and experience 181
  15.10 Record keeping 181
16 Resits, resubmissions and retakes 182
  16.1 Note on terminology 182
  16.2 Rules on resits, resubmissions and retakes 182

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
17 Grading

17.1 Overview
17.2 Internally assessed units
17.3 Externally assessed (examined) units
17.4 Points per grade – unit level
17.5 Final grade for overall qualification
17.6 The ‘Near Pass’ rule

18 Administration arrangements

19 Appendix A: Transferable skills standards and guidance

19.1 Transferable skills – communication standards (oral)
19.2 Transferable skills – communication standards (written)
19.3 Transferable skills – problem-solving standards
19.4 Transferable skills – research standards
19.5 Transferable skills – teamwork standards
1 About these qualifications

These qualifications are Advanced (Level 3) Technical qualifications, on a par with A-levels and have been built in close collaboration with employers and professional bodies ensuring that they have both recognition and value.

They are for learners over the age of 16 who wish to specialise or progress into a specific sector or specific occupational group, through advanced/higher apprenticeships, further study or employment.

Transferable skills (sometimes known as ‘soft skills’) have been contextualised explicitly within the content of each qualification. These transferable skills have been prioritised by employers and professional bodies in this sector and are a mandatory part of the qualification outcome. It is important to note that learners must demonstrate successful achievement of the identified transferable skill(s) appropriate to the qualification on at least one occasion to the required standard.

The Statements of purpose (pages 12 and 19) give more detail on the likely progression for learners with these qualifications.

Each qualification is one of the three components of the new Technical Baccalaureate (TechBacc).

The TechBacc is a performance table measure which recognises the highest level of technical training. It recognises the achievement of learners taking a Technical Level qualification, a Level 3 maths qualification and an Extended Project Qualification (EPQ).
## Qualification at a glance – overview

### 2.1 Level 3 Foundation Technical Level IT: Cyber Security

<table>
<thead>
<tr>
<th>Ofqual qualification number</th>
<th>AQA qualification number</th>
<th>TVQ01010</th>
</tr>
</thead>
<tbody>
<tr>
<td>First registration date</td>
<td>601/7124/8</td>
<td>Age range</td>
</tr>
<tr>
<td>Last registration date</td>
<td>1 September 2015</td>
<td>UCAS points</td>
</tr>
<tr>
<td>Last certification date</td>
<td>31 August 2020</td>
<td>Performance table points</td>
</tr>
<tr>
<td>Total qualification time (TQT)</td>
<td>31 August 2023</td>
<td>Eligibility for funding</td>
</tr>
<tr>
<td></td>
<td>380 (GLH = 360)</td>
<td>Yes</td>
</tr>
<tr>
<td>Unit weighting</td>
<td>(See TQT section for more information)</td>
<td>Entry requirements</td>
</tr>
<tr>
<td>Externally assessed</td>
<td>25% each unit (2 x units)</td>
<td>There are no formal entry requirements for this qualification set by AQA.</td>
</tr>
<tr>
<td>Internally assessed</td>
<td>25% each unit (2 x units)</td>
<td></td>
</tr>
</tbody>
</table>

### Mandatory units

All units in this qualification are mandatory.

### Resits, resubmissions and retakes

The learner is permitted one resit/retake in relation to each unit of the qualification.

Where a unit is examined/externally assessed, this means one resit. Where a unit is internally assessed and externally quality assured, this means one retake.

Resits, resubmissions and retakes are each permitted where learners have both failed the requirements of the unit and where the learner wishes to improve on a grade received.

Any resubmission of an assignment (ie a second attempt at an internally assessed unit task/assignment prior to external quality assurance) must be undertaken without further guidance from the tutor and must be completed within a defined and reasonable period of time following the learner receiving their initial result of the assessment.
Assessment model

This qualification contains externally examined and internally assessed units. Internally assessed units are externally quality assured by AQA.

Examination sessions

January and June each year.

Employer involvement during delivery

It is a requirement that employers are engaged meaningfully in the delivery of this qualification. Further information on this can be found in the individual units (where relevant) and the Meaningful employer involvement section.

Grading

The units are graded Pass, Merit or Distinction

The overall qualification is graded as P, M, D, D*

Transferable skills contextualised within the units of this qualification

These are the skills deemed essential by the employers and professional bodies AQA has collaborated with on the development of this qualification. We have contextualised units around these 'soft' skills. There may be more than one opportunity for each transferable skill to be evidenced to the required standard across the units within the qualification. It is important to note that learners must demonstrate successful achievement of the identified transferable skill(s) appropriate to the qualification on one occasion to the required standard in the identified unit(s). Evidence produced for the transferable skills will be internally assessed and externally quality assured.

- Communication (oral)
- Research
# 2.2 Level 3 Technical Level IT: Cyber Security and Security Administration

<table>
<thead>
<tr>
<th>Ofqual qualification number</th>
<th>AQA qualification number</th>
<th>TVQ01009</th>
</tr>
</thead>
<tbody>
<tr>
<td>First registration date</td>
<td>Age range</td>
<td>16–18, 19+</td>
</tr>
<tr>
<td>Last registration date</td>
<td>UCAS points</td>
<td>Information on UCAS points can be obtained from ucas.com</td>
</tr>
<tr>
<td>Last certification date</td>
<td>Performance table points</td>
<td>Information on performance measures can be found at education.gov.uk</td>
</tr>
<tr>
<td>Total qualification time (TQT)</td>
<td>Eligibility for funding</td>
<td>Yes</td>
</tr>
<tr>
<td>Unit weighting Externally assessed</td>
<td>Entry requirements</td>
<td>There are no formal entry requirements for this qualification set by AQA.</td>
</tr>
<tr>
<td>Internally assessed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.5% each unit (3 x units)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.5% each unit (5 x units)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandatory units</td>
<td>Seven units in this qualification are mandatory, with an option of two (one of which must be studied) to complete the eight units in this programme.</td>
<td></td>
</tr>
<tr>
<td>Resits, resubmissions and retakes</td>
<td>The learner is permitted one resit/retake in relation to each unit of the qualification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where a unit is examined/externally assessed, this means one resit. Where a unit is internally assessed and externally quality assured, this means one retake.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resits, resubmissions and retakes are each permitted where learners have both failed the requirements of the unit and where the learner wishes to improve on a grade received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any resubmission of an assignment (i.e., a second attempt at an internally assessed unit task/assignment prior to external quality assurance) must be undertaken without further guidance from the tutor and must be completed within a defined and reasonable period of time following the learner receiving their initial result of the assessment.</td>
<td></td>
</tr>
</tbody>
</table>
### Assessment model
This qualification contains externally examined and internally assessed units. Internally assessed units are externally quality assured by AQA.

### Examination sessions
January and June each year.

### Employer involvement during delivery
It is a requirement that employers are engaged meaningfully in the delivery of this qualification. Further information on this can be found in the individual units (where relevant) and the Meaningful employer involvement section.

### Grading
The units are graded Pass, Merit or Distinction

The overall qualification is graded as PP, MP, MM, DM, DD, D*D, D*D*

### Transferable skills contextualised within the units of this qualification
These are the skills deemed essential by the employers and professional bodies AQA has collaborated with on the development of this qualification. We have contextualised units around these 'soft' skills. There may be more than one opportunity for each transferable skill to be evidenced to the required standard across the units within the qualification. It is important to note that learners must demonstrate successful achievement of the identified transferable skill(s) appropriate to the qualification on one occasion to the required standard in the identified unit(s). Evidence produced for the transferable skills will be internally assessed and externally quality assured.

- Communication (oral)
- Research
- Problem-solving
3 Level 3 Foundation Technical Level IT: Cyber Security: Statement of purpose

3.1 Qualification objectives

The objectives of this qualification are:

- preparing learners to progress to a qualification in the same subject area but at a higher level or requiring more specific knowledge, skills and understanding
- meeting relevant programmes of learning
- preparing learners for employment
- giving learners personal growth and engagement in learning.

This qualification is linked to the following Standard Occupational Classification (SOC)¹ to prepare learners for work in this area:

AQA Level 3 Foundation Technical Level IT: Cyber Security

- 313 – information technology technicians

3.2 Who is this qualification for?

This technical qualification is aimed at 16 to 18 year-old learners who are seeking to develop skills and access a range of junior cyber security roles in a variety of sector settings, or as the first year of a two year programme where learners aspire to achieve the IT: Cyber Security and Security Administration qualification.

It provides a progression pathway from a range of Level 2 qualifications and learning programmes as can be seen in the following document: gov.uk/government/publications/technical-and-vocational-qualifications-for-14-to-19-year-olds

There are no formal entry requirements for this qualification but to optimise their chances of success, learners will typically have five GCSE's at A* to C, preferably including English and maths.

This qualification could be studied alongside other Level 3 qualifications such as IT: Technical Support, or the IT: Networking or IT: User Support qualifications for a multi-discipline technical role in a small or medium enterprise (SME).

It can form part of a study programme, Technical Baccalaureate and would benefit from being studied alongside an Applied General, A-level or an EPQ.

¹ SOC code is Standard Occupational Category – a common classification of jobs based on their skill content and level – assigned by The Office for National Statistics.
3.3 What does this qualification cover?

All four of the units in this qualification are mandatory and will provide a core knowledge and understanding of IT: Cyber Security. Focusing on computer networks and the development of an understanding of threats and vulnerabilities, all based on underpinning units in the fundamental principles of computing and communication technologies, this qualification will prepare learners to work in this sector.

This qualification has been developed under the guidance of The Tech-Partnership and the British Computer Society (BCS) who are the sectors primary professional bodies.

The learner will cover topics such as:

- how devices communicate, focusing on both physical transmission methods and the media they use
- designing and developing a simple computer network from a user specification and creating a maintenance plan
- the identification and resolution of a range of threats and vulnerabilities.

Transferable skills are those generic ‘soft skills’ that are valued by employers and higher education alike. The following transferable skills have been contextualised into the content of the qualification:

- research
- communication (oral).

Units that provide opportunities to achieve these skills are listed below:

<table>
<thead>
<tr>
<th>Unit code</th>
<th>Unit title</th>
<th>Transferable skill(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>K/507/6427</td>
<td>Developing and maintaining computer networks</td>
<td>Research</td>
</tr>
<tr>
<td>A/507/6433</td>
<td>Network threats and vulnerabilities</td>
<td>Communication (oral)</td>
</tr>
</tbody>
</table>

Opportunities for each available transferable skill will be highlighted in the Pass criteria for the unit where appropriate.

There may be more than one opportunity for each transferable skill to be evidenced to the required standard across the units within the qualification. It is important to note that learners must demonstrate successful achievement of the identified transferable skill(s) appropriate to the qualification on at least one occasion to the required standard.

The Transferable skills standards can be found in Appendix A.

3.4 What could this qualification lead to?

Learners who achieve this qualification will have a range of options.

Progression from this Level 3 Technical qualification is designed to be to work, in a junior cyber security role. Learners would have an opportunity for further study, topping up this qualification to a Level 3 Technical Level in IT: Cyber Security and Security Administration. This qualification will also contribute to university entry and will provide opportunities to undertake a range of professional qualifications from vendors such as CompTIA or CISCO.

However, because it is studied at 16 to 19 as part of the study programme, learners will be studying additional qualifications such as an A-level, an EPQ, an AS and possibly re-sits for GCSE English and/or Maths, learners will potentially be able to access higher education – either HNCs and HNDs or degree programmes.
Therefore, studying this qualification does not restrict future progression into one particular route.

Examples of job opportunities within this sector include:
- IT cyber security administrator, IT cyber security operative.

Companies that might employ someone with this qualification include:
- any company or internet service provider in this sector
- large commercial businesses
- the education sector
- charities.

3.5 Who supports this qualification?

This qualification has been developed in collaboration with employers, professional bodies and key stakeholders in the IT sector. Because of this, the knowledge, skills and competencies gained will provide the best possible opportunity for progression into employment, a higher or advanced apprenticeship or higher education.

This qualification is supported by the following organisations:

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>British Computer Society (BCS)</td>
<td>bcs.org</td>
</tr>
<tr>
<td>The Tech Partnership</td>
<td>thetechpartnership.com</td>
</tr>
<tr>
<td>UK Cyber Security Forum</td>
<td>ukcybersecurityforum.com</td>
</tr>
<tr>
<td>D-RisQ</td>
<td>drisq.com</td>
</tr>
<tr>
<td>Fasthosts</td>
<td>fasthosts.co.uk</td>
</tr>
<tr>
<td>Toshiba UK</td>
<td>toshiba.co.uk</td>
</tr>
<tr>
<td>NETGEAR</td>
<td>netgear.co.uk</td>
</tr>
<tr>
<td>Company</td>
<td>Website</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Weheartdigital Limited</td>
<td>weheart.digital</td>
</tr>
<tr>
<td>CompTIA</td>
<td>comptia.org</td>
</tr>
<tr>
<td>Microsoft</td>
<td>microsoft.com</td>
</tr>
<tr>
<td>AlfaPeople UK</td>
<td>alfapeople.com</td>
</tr>
<tr>
<td>RSPCA</td>
<td>rspca.org.uk</td>
</tr>
<tr>
<td>CCL Group Limited</td>
<td>cclgroup ltd.com</td>
</tr>
<tr>
<td>Cisco</td>
<td>cisco.com</td>
</tr>
<tr>
<td>VMWare IT Academy</td>
<td>vmware.com</td>
</tr>
<tr>
<td>Axelos</td>
<td>axelos.com</td>
</tr>
<tr>
<td>City of Wolverhampton College</td>
<td>wolvcoll.ac.uk</td>
</tr>
<tr>
<td>Burton and South Derbyshire College</td>
<td>bsdac.ac.uk</td>
</tr>
</tbody>
</table>
3.6 What are the benefits of this qualification?

To learners

The UK is now in a situation where very few days will pass without some sort of news article on a breach of IT security somewhere within businesses, the public sector, education, finance or charitable organisations. This often involves data theft, or data loss, as well as intentional acts of sabotage, hacking or other criminal activity. For this reason, the requirement by industry for cyber security staff is on the increase. However, a good cyber security specialist needs to build on a thorough understanding of computers, how they communicate and how networks are put together.

Studying this qualification will give you a variety of options. You could choose to use your achievements to contribute towards the larger IT: Cyber Security and Security Administration programme, or you could use the qualification to contribute towards university entry. Even if you opt to go into an unrelated role in the workplace, this qualification will provide the basic underpinning technical learning that will allow you to help with the organisation’s network, its configuration and its security. This will mean that you have direct or additional skills to offer an employer.

You will study the course as part of a learning programme that could also include other subjects, but will help you to develop the skills and knowledge that are needed in the fast moving IT sector.

You will be working on industry focused assignments to help you prepare for work; this will help you to talk confidently about your knowledge and skills in an interview situation.
When you have successfully completed the course you will be able to look for a job or, if you prefer, you will be able to apply to university or college to continue your studies.

Beginning with the fundamental principles of computing, you will study how computers and devices communicate, how networks are built and maintained, and how to support end users.

**To employers**

This qualification has been developed in consultation with employers and professional bodies who have identified a range of technical and personal skills that are essential for a junior role in this area.

All learners who have achieved this technical qualification will have learned and been assessed using the same content as there are no optional units in this programme and they will have demonstrated and achieved a range of transferable skills that are essential in this area such as the ability to research, solving problems and skills in communication.

Building on the fundamental principles of computing, learners will have studied how computers and devices communicate, how networks are built and maintained, and how to identify and investigate threats and vulnerabilities to computer systems. Moreover, they will have the problem-solving skills to resolve many of these issues.

Therefore, employers can be confident that learners have a solid grounding in technical and personal skills, and in research and communication.

**To higher education institutions**

Discussions with higher education institutions (HEIs) during the development of this IT: Cyber Security qualification identified that to succeed in higher study learners would benefit from basic technical computing skills, particularly if the development of research and communication skills was embedded within the units studied.

Learners will clearly benefit from being able to carry out basic checks on the technologies they use, whether this is connectivity, or issues of security, and being able to resolve many problems as they arise.

In this qualification learners will build on the fundamental principles of computing: they will study how computers and devices communicate, and how networks are built and maintained; they will also understand how to investigate and identify threats and vulnerabilities to systems, with the problem-solving skills to resolve many of these issues.

HEIs can therefore be confident that this qualification will have developed both technical and personal skills necessary to study successfully at a higher level.

### 3.7 Links to professional body memberships

The British Computer Society (BCS) believes employers will recruit and train professionals with AQA Tech-level IT qualifications for roles that are likely to be at registered IT technician level (see Letter of support).
Level 3 Foundation Technical Level IT: Cyber Security: Unit summary

This qualification is made up of four mandatory units. All units must be successfully completed to achieve the full qualification.

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Assessment type</th>
<th>Ofqual unit reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Fundamental principles of computing</td>
<td>External examination</td>
<td>Y/507/6424</td>
</tr>
<tr>
<td>2 Communication technologies</td>
<td>External examination</td>
<td>H/507/6426</td>
</tr>
<tr>
<td>3 Developing and maintaining computer networks</td>
<td>Internally centre assessed</td>
<td>K/507/6427</td>
</tr>
<tr>
<td>4 Network threats and vulnerabilities</td>
<td>Internally centre assessed</td>
<td>A/507/6433</td>
</tr>
</tbody>
</table>

Links with other qualifications

The following unit is shared across all qualifications in the IT sector:
Y/507/6424 1 Fundamental principles of computing

The following units are shared with IT: Networking, IT: User Support, IT: Technical Support and IT: Cyber Security and Security Administration:
H/507/6426 2 Communication technologies
K/507/6427 3 Developing and maintaining computer networks
5 Level 3 Technical Level IT: Cyber Security and Security Administration: Statement of purpose

5.1 Qualification objectives

The objectives of this qualification are:

• preparing learners to progress to a qualification in the same subject area but at a higher level or requiring more specific knowledge, skills and understanding
• meeting relevant programmes of learning
• preparing learners for employment
• supporting a role in the workplace
• giving learners personal growth and engagement in learning.

This qualification is linked to the following Standard Occupational Classification (SOC)\(^2\) to prepare learners for work in this area:

AQA Level 3 Foundation Technical Level IT: Cyber Security and Security Administration

• 2133 – IT specialist managers
• 3131 – IT operations technicians

5.2 Who is this qualification for?

This technical qualification is aimed at 16 to 18 year-old learners who are seeking to develop skills and access a range of networking job roles in a variety of sector settings, or a cyber security apprenticeship.

It provides a progression pathway from a range of Level 2 qualifications and learning programmes as can be seen in the following document: gov.uk/government/publications/technical-and-vocational-qualifications-for-14-to-19-year-olds

There are no formal entry requirements for this qualification but to optimise their chances of success, learners will typically have five GCSE’s at A* to C, preferably including English and maths.

This qualification could be studied alongside other Level 3 qualifications such as User Support for a multi-discipline technical role in a small or medium enterprise (SME).

It can form part of a study programme, Technical Baccalaureate and would benefit from being studied alongside an Applied General, A-level or an EPQ.

---

\(^2\) SOC code is Standard Occupational Category – a common classification of jobs based on their skill content and level – assigned by The Office for National Statistics.
5.3 What does this qualification cover?

Seven of the units in this qualification are mandatory and will provide a core knowledge and understanding of IT: cyber security and security administration. An additional two units are offered—one of which **must** be studied and achieved by the candidate to make up the full eight units required by this programme.

Building on the underpinning units of the fundamental principles of computing, communication technologies and the development and maintenance of a network, learners will explore threats and vulnerabilities, they will consider how identity and access to systems is managed and how network security is administrated. Maths is essential to this pathway and there are opportunities to improve learner’s skills in this area. To complete the qualification learners can choose from two units which have a different focus. Programming for networking and security will provide an opportunity to study the rudiments of programming, focusing more directly on client and server side scripting. Learners will also learn the key features and functions of operating system shell scripting and data encryption. As an alternative, learners could opt to study the Computer forensic investigation unit, which explores the forensic process for gathering information following a cyber security breach. Learners will explore the tools and software used in this environment, undertaking a forensic examination and presenting the evidence using the correct processes and procedures.

This qualification has been developed under the guidance of The Tech-Partnership and the British Computer Society (BCS) who are the sectors primary professional bodies.

The learner will cover topics such as:

- how devices communicate, focusing on both physical transmission methods and the media which they use
- designing and developing a simple computer network from a user specification and creating a maintenance plan
- the identification and resolution of a range of threats and vulnerabilities
- learners will learn how cyber security operatives keep up-to-date on new threats and vulnerabilities, and how administrators record actions taken and planned against maintenance activities.

Transferable skills are those generic ‘soft skills’ that are valued by employers and higher education alike. The following transferable skills have been contextualised into the content of the qualification:

- communication (oral and written)
- research
- problem-solving.

Units that provide opportunities to achieve these skills are listed below:

<table>
<thead>
<tr>
<th>Unit code</th>
<th>Unit title</th>
<th>Transferable skill(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>K/507/6427</td>
<td>Developing and maintaining computer networks</td>
<td>Research</td>
</tr>
<tr>
<td>A/507/6433</td>
<td>Network threats and vulnerabilities</td>
<td>Communication (oral)</td>
</tr>
<tr>
<td>Y/507/6438</td>
<td>Managing identity and access to systems</td>
<td>Problem-solving</td>
</tr>
<tr>
<td>R/507/6440</td>
<td>Computer forensic investigation</td>
<td>Communication (oral)</td>
</tr>
</tbody>
</table>

Opportunities for each available transferable skill will be highlighted in the pass criteria for the unit where appropriate.

There may be more than one opportunity for each transferable skill to be evidenced to the required standard across the units within the qualification. It is important to note that learners **must** demonstrate successful achievement of the identified transferable skill(s) appropriate to the qualification on at least **one** occasion to the required standard.

Visit [aqa.org.uk](http://aqa.org.uk) for the most up-to-date specification, resources, support and administration.
The Transferable skills standards can be found in Appendix A.

5.4 What could this qualification lead to?

Learners who achieve this qualification will have a range of options.

Progression from this Level 3 Technical qualification is designed to be to work, in a junior cyber security role. This qualification will also contribute to university entry and will provide opportunities to undertake a range of professional qualifications from vendors such as CompTIA or CISCO.

However, as it is studied at 16 to 19 as part of the study programme, learners will be studying additional qualifications such as an A-level, an EPQ, an AS and possibly re-sits for GCSE English and/or Maths, learners will potentially be able to access higher education – either HNCs and HNDs or degree programmes.

Therefore, studying this qualification does not restrict future progression into one particular route.

The following are examples of job opportunities within this sector:
- IT cyber security administrator
- IT cyber security technician.

Companies that might employ someone with this qualification include:
- any company or internet service provider in this sector
- large commercial businesses
- the education sector
- charities.

5.5 Who supports this qualification?

This qualification has been developed in collaboration with employers, professional bodies and key stakeholders in the IT sector. Because of this, the knowledge, skills and competencies gained will provide the best possible opportunity for progression into employment, a higher or advanced apprenticeship or higher education.

This qualification is supported by the following organisations:

<table>
<thead>
<tr>
<th>British Computer Society (BCS)</th>
<th>bcs.org</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Tech Partnership</td>
<td>thetechpartnership.com</td>
</tr>
<tr>
<td>UK Cyber Security Forum</td>
<td>ukcybersecurityforum.com</td>
</tr>
<tr>
<td>Logo</td>
<td>Company</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td><img src="D-RisQ.png" alt="D-RisQ" /></td>
<td>D-RisQ</td>
</tr>
<tr>
<td><img src="Fasthosts.png" alt="Fasthosts" /></td>
<td>Fasthosts</td>
</tr>
<tr>
<td>![Toshiba UK](Toshiba UK.png)</td>
<td>Toshiba UK</td>
</tr>
<tr>
<td><img src="NETGEAR.png" alt="NETGEAR" /></td>
<td>NETGEAR</td>
</tr>
<tr>
<td>![Weheartdigital Limited](Weheartdigital Limited.png)</td>
<td>Weheartdigital Limited</td>
</tr>
<tr>
<td><img src="CompTIA.png" alt="CompTIA" /></td>
<td>CompTIA</td>
</tr>
<tr>
<td><img src="Microsoft.png" alt="Microsoft" /></td>
<td>Microsoft</td>
</tr>
<tr>
<td>![AlfaPeople UK](AlfaPeople UK.png)</td>
<td>AlfaPeople UK</td>
</tr>
<tr>
<td><img src="RSPCA.png" alt="RSPCA" /></td>
<td>RSPCA</td>
</tr>
<tr>
<td>![CCL Group Limited](CCL Group Limited.png)</td>
<td>CCL Group Limited</td>
</tr>
<tr>
<td><img src="Cisco.png" alt="Cisco" /></td>
<td>Cisco</td>
</tr>
<tr>
<td>![VMWare IT Academy](VMWare IT Academy.png)</td>
<td>VMWare IT Academy</td>
</tr>
<tr>
<td>Institution</td>
<td>Website</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Axelos</td>
<td>axelos.com</td>
</tr>
<tr>
<td>City of Wolverhampton College</td>
<td>wolvcoll.ac.uk</td>
</tr>
<tr>
<td>Burton and South Derbyshire College</td>
<td>bsdc.ac.uk</td>
</tr>
<tr>
<td>Solihull College</td>
<td>solihull.ac.uk</td>
</tr>
<tr>
<td>South and City College Birmingham</td>
<td>sccb.ac.uk</td>
</tr>
<tr>
<td>Newcastle-under-Lyme College</td>
<td>nulc.ac.uk</td>
</tr>
<tr>
<td>Edge Hill University</td>
<td>edgehill.ac.uk</td>
</tr>
<tr>
<td>University of Bedfordshire</td>
<td>beds.ac.uk</td>
</tr>
<tr>
<td>Staffordshire University</td>
<td>staffs.ac.uk</td>
</tr>
</tbody>
</table>
5.6 What are the benefits of this qualification?

To learners
Cyber security is now the focus of many organisations in the UK, Europe and the wider world. This is because a system that is vulnerable risks damaging an organisation’s ability to operate as well as threatening its reputation. For this reason, the requirement by industry for cyber security staff is on the increase. However, a good cyber security specialist needs to build on a thorough understanding of computers, how they communicate and how networks are put together.

This qualification is currently the only technical qualification that has optional units. You will study seven mandatory units and will have the choice of Programming for networking and security or Computer forensic investigation, depending on your subsequent aspirations. You will need to achieve eight units overall.

Studying this qualification will give you a variety of options. You will be able to access junior cyber security roles, or access a Level 4 apprenticeship or Trailblazer Apprenticeship as a Cyber Security Analyst. You could also choose to use your achievements to contribute towards university entry.

You will study the course as part of a learning programme that could also include other subjects, but will help you to develop the skills and knowledge that are needed in the fast moving IT sector.

You will be working on industry focused assignments to help you to prepare for work; this will help you to talk confidently about your knowledge and skills in an interview situation.

When you have successfully completed the course you will be able to look for a job, or if you prefer, along with your other studies you will be able to apply to university or college to continue your studies.

To employers
This qualification has been developed in consultation with employers and professional bodies who have identified a range of technical and personal skills that are essential for a junior role in this area.

All learners who have achieved this technical qualification will have learned and been assessed using the same content. There are, however, two optional units, one of which must be studied to complete the qualification. Learners will have demonstrated and achieved a range of transferable skills that are essential in this area such as the ability to research and skills in communication.

Building on the fundamental principles of computing, learners will have studied how computers and devices communicate, how networks are built and maintained and they will understand how to investigate and identify threats and vulnerabilities to computer systems, with the problem-solving skills to resolve many of these issues. Learners will understand how networks are administrated and how to ensure that the organisation’s network maintains secure at all times. Having studied seven mandatory units, learners will have had an option of two, one of which must be successfully achieved to complete the qualification. These are Programming for networking and security or Computer forensic investigation. Each of the units has its value – programming for those who wish to administrate organisational systems, and forensic investigation for those who seek a forensic role for public sector organisations and supporting businesses.

Employers can therefore be confident that learners have a solid grounding in technical and personal skills in research, problem-solving and communication.
To higher education institutions

Discussions with higher education institutions (HEIs) during the development of this IT: Cyber security and security administration qualification identified that to succeed in higher study learners would benefit from basic technical computing skills, particularly if the units studied also had embedded research, problem-solving and communication skills development.

Learners will clearly benefit from being able to carry out basic checks on the technologies they use, whether this is connectivity, or issues of security, being able to resolve many problems as they arise.

Building on the fundamental principles of computing, learners will have studied how computers and devices communicate, how networks are built and maintained and they will understand how to investigate and identify threats and vulnerabilities to computer systems, with the problem-solving skills to resolve many of these issues. Learners will understand how networks are administrated and how to ensure that the organisation’s network maintains secure at all times. Having studied seven mandatory units, learners will have had an option of two, one of which must be studied and achieved to complete the qualification. These are Programming for networking and security or Computer forensic investigation. Each of the units has its value – programming for those who wish to administrate organisational systems, and forensic investigation for those who seek a forensic role for public sector organisations and supporting businesses.

HEIs can therefore be confident that this qualification will have developed both technical and personal skills necessary to study successfully at a higher level.

5.7 Links to trailblazers

This qualification has been developed to provide a comprehensive grounding in Cyber Security with a view to offer learners the opportunity to progress to a Level 4 Trailblazer Apprenticeship as a Cyber Security Professional (currently planned for 2015/16): thetechpartnership.com/news-events/announcement-listing/trailblazer-apprenticeships-for-cyber-security

5.8 Links to professional body memberships

The British Computer Society (BCS) believes employers will recruit and train professionals with AQA Tech-level IT qualifications for roles that are likely to be at registered IT technician level (see Letter of support).
6 Level 3 Technical Level IT: Cyber Security and Security Administration: Unit summary

This qualification is made up of seven mandatory units and two optional units (one of which must be studied and achieved). All units must be successfully completed to achieve the full qualification.

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Assessment type</th>
<th>Ofqual unit reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Fundamental principles of computing</td>
<td>External examination</td>
<td>Y/507/6424</td>
</tr>
<tr>
<td>2 Communication technologies</td>
<td>External examination</td>
<td>H/507/6426</td>
</tr>
<tr>
<td>3 Developing and maintaining computer networks</td>
<td>Internally centre assessed</td>
<td>K/507/6427</td>
</tr>
<tr>
<td>4 Network threats and vulnerabilities</td>
<td>Internally centre assessed</td>
<td>A/507/6433</td>
</tr>
<tr>
<td>5 Maths for computing</td>
<td>Internally centre assessed</td>
<td>R/507/6437</td>
</tr>
<tr>
<td>6 Network and cyber security administration</td>
<td>External examination</td>
<td>J/507/6435</td>
</tr>
<tr>
<td>7 Managing identity and access to systems</td>
<td>Internally centre assessed</td>
<td>Y/507/6438</td>
</tr>
<tr>
<td>8 Programming for networking and security *</td>
<td>Internally centre assessed</td>
<td>D/507/6439</td>
</tr>
<tr>
<td>9 Computer forensic investigation *</td>
<td>Internally centre assessed</td>
<td>R/507/6440</td>
</tr>
</tbody>
</table>

*Units 8 and 9 are optional – but one must be studied and successfully achieved as part of this programme.

Links with other qualifications

The following unit is shared across the IT sector:
Y/507/6424  1  Fundamental principles of computing

The following units are shared with IT: Networking, IT: User Support, IT: Cyber Security and IT: Technical Support:
H/507/6426  2  Communication technologies
K/507/6427  3  Developing and maintaining computer networks

The following unit is shared with IT: User Support:
R/507/6440  9  Computer forensic investigation

The following unit is also shared with IT: Networking:
R/507/6437  5  Maths for computing
7 Meaningful employer involvement

7.1 Introduction

It is important that centres develop an approach to teaching and learning that supports the assessment of the technical focus of a Tech-level qualification. The specification contains a balance of practical skills and knowledge requirements and centres need to ensure that appropriate links are made between theory and practice in a way that is relevant to the occupational sector.

This will require the development of relevant and up-to-date training materials that allow learners to apply their learning to actual events and activity within the sector, and to generate appropriate evidence for their portfolio.

It is a requirement that employers are involved in the delivery and/or assessment of the Tech-level to provide a clear ‘line of sight’ to work, advanced/higher apprenticeships or higher education. Employer engagement enriches learning, raises the credibility of the qualification in the eyes of employers, parents and learners – as well as also furthering the critical collaboration between the learning and skills sector and industry.

It is therefore a requirement that all learners undertake meaningful activity involving employers during their study and this activity will be scrutinised as part of our ongoing quality assurance activities with centres.

Such is the importance of meaningful employer involvement in the delivery of this qualification, should a centre be unable to evidence this, we will impose a sanction, together with an associated action plan. Further information on this process can be found in the AQA Centre Administration Guide for Technical and Vocational Qualifications.

AQA will not stipulate the minimum duration or contribution of employer involvement to the overall qualification grade as it is important that centres and employers are allowed flexibility in how best to work together to support learning and in which units – but this collaboration must be significant.

7.2 Definition of meaningful employer involvement

In order to meet our requirements, meaningful employer involvement must take at least one of the following forms:

- learners undertake structured work experience or work placements that develop skills and knowledge relevant to this qualification
- learners undertake project work, exercises and/or assessments set with input from industry practitioners – such as getting employers involved in developing real life case studies, or assignments
- learners take one or more units delivered or co-delivered by an industry practitioner – this could be in the form of masterclasses or guest lectures
- industry practitioners operating as ‘expert witnesses’ that contribute to the assessment of a learner’s work or practice, operating within a specified assessment framework. This may be for specific project work, exercises or examinations, or all assessments for a qualification.
For the purpose of clarity, the following activities, whilst valuable, would **not** be considered as meaningful employer involvement:

- employers hosting visits, providing premises, facilities or equipment
- employers or industry practitioners providing talks or contributing to delivery on employability, general careers advice, CV writing, interview training
- learner attendance at career fairs, events or other networking opportunities
- simulated or centre-based working environments
- employers providing learners with job references.

More information on employer involvement in the delivery of technical level qualifications can be found at:


### 7.3 Employer involvement in quality assurance

We need to make sure that the assessment remains relevant and valid, and that learning outcomes are what employers and higher education institutions are expecting of a learner who has achieved a Level 3 Tech-level qualification.

Each year a panel, including representatives from employers and HE, will be brought together to review outcomes from the units and we will ask for samples of learner work from your centre at each AQA external quality assurer (EQA) visit.

We are keen to work collaboratively with employers and HE to make sure that whatever the progression route chosen by the learner, this qualification will be recognised and valued.

If you have a local employer that would like to be involved in this review, we would be very pleased to consider them. Please email their contact details to techlevels@aqa.org.uk
8 Synoptic delivery and assessment

The definition of synoptic assessment used by AQA is:
‘A form of assessment which requires a learner to demonstrate that they can identify and use effectively, in an integrated way, an appropriate selection of skills, techniques, concepts, theories, and knowledge from across the whole qualification or unit, which are relevant to a key task’.

The design of this qualification allows learners to develop knowledge, understanding and skills from some units and then evidence this learning in the performance outcomes contained within other units.

The significant amount of synoptic content within the Tech-level supports synoptic learning and assessment by:
• showing teaching and learning links between the units across the specification
• giving guidance or amplification relating to the grading criteria for the internally assessed units, about where learners could apply the knowledge and understanding from other units
• providing a coherent learning programme of related units
• allowing holistic delivery and the application of prior or concurrent learning
• providing opportunities for the learning and assessment of multiple units combined together to promote holistic delivery
• developing and assessing learners’ use of transferable skills in different contexts.

Whilst we do not prescribe in which order the units should be delivered or assessed, it is important for centres to be aware of the links between the units so that the teaching, learning and assessment can be planned accordingly. This way, when being assessed, learners can apply their learning in ways which show they are able to make connections across the qualification.

It is therefore a requirement that all learners undertake meaningful synoptic learning and assessment during their study. Plans for how this will be undertaken will be scrutinised as part of our centre approval process and its implementation monitored during our ongoing quality assurance activities with centres.

Within each unit we provide references to where the unit content maps from or to other units within the qualification. This will help the learner understand where there are explicit opportunities for synoptic learning as well as synoptic assessment.

For example, learners will be able to see very clearly how they can apply the underpinning knowledge and theory from the core units into real life or work related tasks – such as projects and work experience – within the specialist units.

This approach will also enable learners to integrate transferable skills much valued by employers and HE into their assignments.
The following grid demonstrates the overall synoptic coverage in each unit of the qualification:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Assessment outcomes/pass criteria</th>
<th>Synoptic links to other units</th>
<th>% of synoptic assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fundamental principles of computing</td>
<td>5</td>
<td>Underpinning knowledge for sector</td>
<td>5/5 (100%)</td>
</tr>
<tr>
<td>Communication technologies</td>
<td>5</td>
<td>Underpinning knowledge for pathway</td>
<td>5/5 (100%)</td>
</tr>
<tr>
<td>Developing and maintaining computer networks</td>
<td>14</td>
<td>Linked to Units 1, 2, and 5</td>
<td>7/14 (50%)</td>
</tr>
<tr>
<td>Network threats and vulnerabilities</td>
<td>15</td>
<td>Linked to Units 1, 2, 3, 6, 7 and 8</td>
<td>11/16 (69%)</td>
</tr>
<tr>
<td>Maths for computing</td>
<td>15</td>
<td>Linked to Units 1, 2 and 6</td>
<td>9/15 (60%)</td>
</tr>
<tr>
<td>Network and cyber security administration</td>
<td>7</td>
<td>Linked to Units 1, 2, 3, 4, 5, 7, 8 and 9</td>
<td>5/7 (72%)</td>
</tr>
<tr>
<td>Managing identity and access to systems</td>
<td>15</td>
<td>Linked to Units 1, 2, 3, 4, 5 and 6</td>
<td>12/15 (80%)</td>
</tr>
<tr>
<td>Programming for networking and security</td>
<td>16</td>
<td>Linked to Units 1, 3, 4, 5, 6 and 7</td>
<td>8/16 (50%)</td>
</tr>
<tr>
<td>Computer forensic investigation</td>
<td>12</td>
<td>Linked to Units 1 and 4</td>
<td>5/12 (42%)</td>
</tr>
</tbody>
</table>

This qualification contains 72.6% synopticity calculated over all eight units where the Programming for network and security has been used, or 71.6% synopticity calculated over all eight units where the Computer forensic investigation has been used.
9 Total qualification time

For any qualification which it makes available, Ofqual requires an awarding organisation to:

a assign a number of hours for total qualification time to that qualification, and
b assign a number of hours for guided learning to that qualification.

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

Total qualification time is comprised of the following two elements:

a the number of hours which an awarding organisation has assigned to a qualification for guided learning (GLH)
   AQA has assigned GLH to the overall qualification and the individual units.

b 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.

AQA has assigned the following GLH and TQT values to its qualifications:

<table>
<thead>
<tr>
<th>Qualification</th>
<th>Guided learning hours (GLH)</th>
<th>Total qualification time (TQT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT: Cyber Security (TVQ01010)</td>
<td>360</td>
<td>380</td>
</tr>
<tr>
<td>IT: Cyber Security and security administration (TVQ01009)</td>
<td>720</td>
<td>760</td>
</tr>
</tbody>
</table>
10 Transferable skills

These valued ‘employability’ skills are an integral and explicit element within the design and structure of all AQA Level 3 Technical Level qualifications.

Discussions and collaboration with centres, employers and stakeholders (such as further education (FE) colleges, university technical colleges (UTCs), sector skills councils, professional/trade bodies and HE), made it clear that the inclusion of these skills is regarded as a priority, and that they should be included through contextualisation within the core subject content.

Employers and stakeholders prioritised the skills they required from employees in the sector as follows:
- communication
- problem-solving
- research.

Rather than force the inclusion of these skills across a random selection of units or across the qualification as a whole, specific units have been identified as being most appropriate and suitable for the inclusion of a transferable skill within the subject context. The skill becomes the driver for the assessment – rather than the subject content and this will be demonstrated by producing evidence to meet the required standard³. Not every unit within the qualification has a skill contextualised within the subject content.

<table>
<thead>
<tr>
<th>Unit code</th>
<th>Pathway</th>
<th>Unit title</th>
<th>Transferable skill(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>K/507/6427</td>
<td>Cyber Security</td>
<td>Developing and maintaining computer networks</td>
<td>Research</td>
</tr>
<tr>
<td></td>
<td>Cyber Security and Security Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K/506/6111</td>
<td>Cyber Security</td>
<td>Managing threats and vulnerabilities</td>
<td>Communication (oral)</td>
</tr>
<tr>
<td></td>
<td>Cyber Security and Security Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R/507/6440</td>
<td>Cyber Security and Security Administration</td>
<td>Computer forensic investigation</td>
<td>Communication (oral)</td>
</tr>
<tr>
<td>Y/507/6438</td>
<td>Cyber Security and Security Administration</td>
<td>Managing identity and access to systems</td>
<td>Problem-solving</td>
</tr>
</tbody>
</table>

The skill is assessed as a performance outcome of the unit, at the Pass grade. It is assessed in the same way as any other assessment criteria within the unit.

The formal inclusion of a contextualised transferable skill does not preclude the inclusion of other ‘soft’ or ‘employability’ skills within the unit at the point of delivery, for example those which employers and HE will also value, such as critical thinking, project management, leadership, time management etc. However, these additional ‘employability’ skills will not be formally assessed as part of the unit performance outcomes.

³ Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.
The AQA Skills statement

Upon the successful completion of a qualification, each learner will be issued with a Skills statement that will sit alongside their formal qualification certificate.

This Skills statement records the transferable skills that were contextualised within the units of the qualification and is an explicit way for learners to showcase the skills that have been formally assessed as part of the qualification. This Skills statement can then be used by a learner as evidence of this achievement within their CVs or HE applications.
The following delivery resources and support materials are available from AQA.

- A full Scheme of work (SOW) has been provided for each of the units in this programme. The SOW breaks down the unit content across a 30 teaching week academic year, although this is not mandated. Suggestions have been made for activities both for the tutor and the learner, and the document also contains links to external resources such as videos, task sheets, pdfs, PowerPoint presentations etc. Opportunities to develop English and maths skills have been identified and flagged, and SOWs include some mapping for stretch and challenge and equality and diversity, although tutors will benefit from making this much more class relevant. Assignment handouts have been identified and the assessment points for transferable skills have been highlighted in the final column.

- A sample Lesson plan has also been provided against the SOW, as a guide for good practice.

- A sample assignment has been provided for each of the internally assessed units. These are not mandated in the assessment of this qualification, but do provide a good starting point to help tutors who would benefit from assessment support. These assessments do not necessarily cover all of the criteria that need to be assessed within a unit and it is the tutor’s responsibility to ensure that all criteria are assessed across the unit and qualification.

- Sample question papers and mark schemes for each of the examined units.

The schemes of work and lesson plans are available at: aqa.org.uk/subjects/ict-and-computer-science/tech-level/it-cybersecurity/teaching-resources

The sample assessment materials (question papers and mark schemes), plus the available sample assignments can be found at: aqa.org.uk/subjects/ict-and-computer-science/tech-level/it-cybersecurity/assessment-resources
12 Qualification units

12.1 Unit 1: Fundamental principles of computing

<table>
<thead>
<tr>
<th>Title</th>
<th>Fundamental principles of computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>Y/507/6424</td>
</tr>
<tr>
<td>Assessment</td>
<td>Externally assessed</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>N/A</td>
</tr>
<tr>
<td>Resources required for this unit</td>
<td>Central processing unit (CPU); memory chips; motherboards; internal disk drives; expansion cards; computer cases; cables; power supplies; cooling devices; ports; external devices; operating systems; device drivers; applications software.</td>
</tr>
<tr>
<td>Synoptic assessment within this unit</td>
<td>This unit provides the underpinning knowledge for all units contained in either the IT: Cyber Security pathway or the IT: Cyber Security and Security Administration pathway.</td>
</tr>
</tbody>
</table>

Aim and purpose
This unit will provide the learner with the necessary knowledge to understand the different hardware and elements of a computer system and how these contribute to a fully functioning computer system. The learner will also develop a range of skills required to make changes to computer systems to ensure that they are fit for the particular requirements of the users.

Unit introduction
The fundamental requirement of any information system is a responsive computer system. Anyone who works in the IT industry needs to be fully conversant with the hardware and software elements that work together to meet the needs of the user.

This unit will provide the learner with understanding of the fundamental building blocks of such systems and enable them to understand how the various components can be linked together and why different possible combinations of these elements can affect the potential of the system to perform to the required standard.

The ability to test or upgrade a system to identify any problems and ensure that it continues to provide the required level of performance is a fundamental skill required of a computer technician. This unit will also provide the opportunity for the learner to develop the relevant skills to enable them to carry out a range of basic tests and make the necessary adjustments to the system for a given scenario.

While small systems may be managed and maintained by a single individual, larger systems require teams of specialists to take responsibility for one or more components in areas such as security. Whether large or small, it is necessary for all testing and adjustments to the systems to be recorded and reported to the responsible manager. As a result, this unit will provide learners with opportunities to develop their skills in teamworking, written and oral communication and problem-solving.
Computer systems use electricity and some components are heavy and/or difficult to handle, so the learner will be required to understand the correct methods for working safely with electrical equipment, and avoiding damage to components through static electricity. All computer systems use data, some (if not all) of which will be sensitive and the learners will need to understand their responsibilities in protecting the data and systems. Therefore, the learner will need to identify and apply the relevant laws and regulations governing working with electrical systems. It is essential that learners consider the safe disposal of equipment, manual lifting, data protection and computer misuse, and that they carry out risk assessments before undertaking any activities such as dismantling computers, moving computers, etc.

Unit content

<table>
<thead>
<tr>
<th>Different types of computer</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal computers</td>
<td>Micro-computers, tablets.</td>
</tr>
<tr>
<td></td>
<td>Single user.</td>
</tr>
<tr>
<td></td>
<td>Applications for personal use eg email, diary, spreadsheets, databases, word processors, web access.</td>
</tr>
<tr>
<td>Multi-user computers</td>
<td>Mainframes.</td>
</tr>
<tr>
<td></td>
<td>Supercomputers.</td>
</tr>
<tr>
<td></td>
<td>Multi-user.</td>
</tr>
<tr>
<td></td>
<td>Applications for governments and research eg storing and manipulating large volumes of data for online bookings and enquiries, payroll, weather prediction, simulators.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware components of a computer system</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The internal components of a computer</td>
<td>Arithmetic logic unit (ALU).</td>
</tr>
<tr>
<td>CPU</td>
<td>Main memory.</td>
</tr>
<tr>
<td></td>
<td>Cache.</td>
</tr>
<tr>
<td></td>
<td>Control unit.</td>
</tr>
<tr>
<td></td>
<td>Registers; accumulator etc.</td>
</tr>
<tr>
<td></td>
<td>The steps of the Fetch-Execute Cycle.</td>
</tr>
<tr>
<td></td>
<td>The effect of an interrupt on a Fetch-Execute Cycle.</td>
</tr>
<tr>
<td></td>
<td>Pipelines.</td>
</tr>
<tr>
<td></td>
<td>Multi-core processors.</td>
</tr>
</tbody>
</table>
## Hardware components of a computer system

<table>
<thead>
<tr>
<th>The internal components of a computer</th>
<th>Non-CPU components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply units (PSUs) which convert power from alternating current (AC) to direct current (DC).</td>
<td>• Cooling devices:</td>
</tr>
<tr>
<td>• Cooling devices:</td>
<td>• fans</td>
</tr>
<tr>
<td>• heat sinks and thermal paste</td>
<td>• water-based.</td>
</tr>
<tr>
<td>• water-based.</td>
<td>• Internal hard drives.</td>
</tr>
<tr>
<td>• Memory chips:</td>
<td>• Memory chips:</td>
</tr>
<tr>
<td>• Random Access Memory (RAM) eg Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM)</td>
<td>• Random Access Memory (RAM) eg Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM)</td>
</tr>
<tr>
<td>• Read Only Memory (ROM)</td>
<td>• Read Only Memory (ROM)</td>
</tr>
<tr>
<td>• Programmable Read Only Memory (PROM)</td>
<td>• Programmable Read Only Memory (PROM)</td>
</tr>
<tr>
<td>• Erasable Programmable Read Only Memory (EPROM)</td>
<td>• Erasable Programmable Read Only Memory (EPROM)</td>
</tr>
<tr>
<td>• Electrical Erasable Programmable Read Only Memory (EEPROM).</td>
<td>• Electrical Erasable Programmable Read Only Memory (EEPROM).</td>
</tr>
<tr>
<td>• Basic Input Output System (BIOS) and Extensible Firmware Interface (EFI):</td>
<td>• Basic Input Output System (BIOS) and Extensible Firmware Interface (EFI):</td>
</tr>
<tr>
<td>• independent of operating system</td>
<td>• instructions eg booting, identification of devices, cpu, memory, power-on self-test (post).</td>
</tr>
<tr>
<td>• Cards or expansion cards such as sound, graphics, network cards etc.</td>
<td>• Cards or expansion cards such as sound, graphics, network cards etc.</td>
</tr>
<tr>
<td>• Input/output controllers.</td>
<td>• Input/output controllers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication methods</th>
<th>External hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer ports such as Universal Serial Bus (USB), FireWire, Serial Advanced Technology Attachment (SATA), parallel.</td>
<td>• Input devices eg mouse, scanner, keyboard, touch screen, web cam, microphone, barcode reader, sensors.</td>
</tr>
<tr>
<td>Internal and external computer buses eg systems bus, data bus, memory bus, parallel bus, serial bus.</td>
<td>• Biometric readers eg fingerprint, iris.</td>
</tr>
<tr>
<td></td>
<td>• External output devices eg printers (2D, 3D), screens, speakers, slide projectors.</td>
</tr>
<tr>
<td></td>
<td>• Secondary/backing storage eg hard disk drives, USB drives, read/writeable DVDs, removable magnet disks, fixed magnetic disks, solid state drives.</td>
</tr>
<tr>
<td></td>
<td>• Specialist operator console.</td>
</tr>
</tbody>
</table>

## Software requirements of a computer system

<table>
<thead>
<tr>
<th>Types of software</th>
<th>• Systems software.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Applications software.</td>
</tr>
<tr>
<td></td>
<td>• Shareware.</td>
</tr>
<tr>
<td></td>
<td>• Freeware.</td>
</tr>
<tr>
<td></td>
<td>• Open source.</td>
</tr>
</tbody>
</table>
## Software requirements of a computer system

### System software
- Libraries eg routines which are used by multiple programs.
- Utility programs – such as systems backup, systems optimisers, disk formatters, disk defragging, text editor, graphic editor etc.
- Systems management software notifying actual or impending failures, capacity issues and other systems and network events eg monitoring, controlling and reporting on status of:
  - client devices (PC, laptop, other mobile devices)
  - printers
  - storage.

### Operating systems
- A range of operating systems eg Microsoft Windows, Apple Mac OSX, Android, Linux, Unix.
- Types of operating systems eg single user, multi-user, multiprocessing, multitasking (co-operative and pre-emptive), multi-threading operating systems.
- Operating system functions eg input recognition, output device recognition, tracking files, tracking directories, managing peripheral devices, sharing resources between users, ensuring that users do not interfere with each other, managing security, access to devices, programs and data.

### Device drivers
- Types of device driver.
- Role eg linking devices to computer system, translating commands received from operating system.
- Devices requiring drivers eg expansion cards (eg network, sound, video card), printers, monitors, scanners, mobile devices.

### Applications software
- Types of application software:
  - off-the-shelf: generic programs which provide a recognised business or personal need eg word processors, databases, computer games, spreadsheets, email, internet software..
  - bespoke designed for specific client needs..
  - tailored – off-the-shelf adjusted for specific client needs.

### Security software
- Firewalls.
- Antivirus.
- Anti-spyware.
- Authorisation.
- Authentication.
- Biometrics.
- Encryption.

### Software inventory
- Software name.
- Software version.
- Date.
- Activity eg installation, test, update.
- Outcomes eg successful, failure, reasons for failure (if appropriate), remedial steps taken.
- Report of any other observations.
### How data is converted to information

| Data | Elements which can be processed to produce useful information eg numbers (numeric), characters (alphanumeric), images, signals.  
|      | Qualitative and quantitative data. |
| Information | Organised data which delivers knowledge, clarification or proof eg reports, charts, graphs, telephone directories, text books.  
| | Information characteristics:  
| | accuracy  
| | validity  
| | timeliness  
| | authority  
| | objectivity. |

### Data processing cycle

| Input data eg words, numbers, images, signals.  
| Arithmetic operations eg +, -, *, /  
| Logical eg ‘and’, ‘or’, ‘not’, ‘nand’, ‘xor’  
| Output information eg printed report, on-screen email, correction or operating signals to machinery. |

### How computers process user requirements

| Data storage units | Bits, nibbles, bytes and words.  
| Common multiples, eg:  
| kilobyte  
| megabyte  
| gigabyte  
| terabyte  
| petabyte.  
| International system of quantities ‘Kibibyte’, etc and conflict with inaccurate international system of units (SI) definition of ‘Kilo’, etc. |

| Character encoding | Character encoding eg American Standard Code for Information Interchange (ASCII), Extended ASCII, Unicode. |

| Programming languages | Natural languages, eg English, French etc.  
| Man readable vs computer readable languages (ie binary).  
| Low level languages:  
| machine code  
| assembly language.  
| High level languages which use commands and comments as well as characters which are easier for humans to understand eg JavaScript, C++, VB.net, Ada, Fortran, Delphi, PHP, Python.  
| Fourth Generation languages (4GL) clear human commands eg Structured Query Language (SQL), OpenEdge Advanced Business Language, PROLOG. |

| Converting source code to machine code | Assemblers, including cross-assemblers.  
| Translators and their differences:  
| interpreters  
| compilers. |
Assessment outcomes

Learners will be able to:

### Assessment outcome 1: Understand the different types of computer

- a. The features of personal computers.
- b. The features of applications for personal use and their uses.
- c. The features of multi-user computers.
- d. The features of applications for governments and research used for storing and manipulating large volumes of data.

### Assessment outcome 2: Understand the hardware requirements of a computer system

- a. The internal components of a CPU including their purpose.
- b. The steps of the Fetch-Execute Cycle.
- c. The effect and purpose of an interrupt on a Fetch-Execute Cycle.
- d. Maskable interrupts (IRQ) and non-maskable interrupts (NMI).
- e. The internal components of a computer.
- f. Internal and external power supply units (PSUs) which convert power from alternating current (AC) to direct current (DC).
- g. Cooling devices and their purpose.
- h. How internal hard drives work.
- i. Types of memory chips.
- j. Basic input output system (BIOS) and Extensible firmware interface (EFI) and their purpose.
- k. Input/output controllers and expansion cards such as sound, graphics, network cards etc. and their purpose.
- l. Computer ports and their purpose.
- m. Internal and external computer buses.
- n. Input devices eg mouse, scanner, keyboard, touch screen, web cam, microphone, barcode reader, sensors, biometric readers eg fingerprint, iris.
- o. External output devices eg printers (2D, 3D), screens, speakers, slide projectors.
- p. Secondary/backing storage eg hard disk drives, USB drives, read/writeable DVDs, removable magnetic disks, fixed magnetic disks, solid state drives (SSD).
- q. The purpose of specialist operator consoles.

### Assessment outcome 3: Understand the software requirements of a computer system

- a. Types of software.
- b. Advantages and disadvantages of shareware, freeware and open source software.
- c. The purpose of libraries eg routines which are used by multiple programs.
- d. The features and purpose of utility programs.
- e. The role of systems management software notifying actual or impending failures, capacity issues and other systems and network events eg monitoring, controlling and reporting on status.
- f. The purpose of client devices.
- g. Types of operating systems and their function.
- h. The purpose of the operating systems.
Assessment outcome 3: Understand the software requirements of a computer system

i. The purpose of access to operating systems via a command line interface (CLI).

j. Types of file storage.

k. Justify the use of different types of file storage.

l. The purpose of device drivers.

m. The features of anti-malware and their purpose.

n. Security methods and their purpose.

o. The role of the software inventory including the following records.

Assessment outcome 4: Understand how data is converted to information

a. The terms data and information with examples.

b. Methods of conveying information.

c. What can affect the quality or validity of information.

d. Qualitative and quantitative data.

e. The input, process, output cycle.

f. Arithmetic operations +, -, *, /

g. Logical operations.

h. Truth tables using up to three logical operations.

Assessment outcome 5: Demonstrate how computers process user requirements

a. Bits, nibbles, bytes and words.

b. Use common multiples represented by decimal numbers or powers of 10.

c. The International System of Quantities ‘Kibibyte’, etc and the International System of Units (SI) definition of ‘Kilo’ etc.

d. The features and purpose of character encoding.

e. Types of language.

f. Describe Low level languages and their purpose.

g. The features and purpose of high level languages.

h. The features and purpose of Fourth Generation languages (4GL).

i. The purpose of assemblers, including cross-assemblers.

j. The features and purpose of translators.

Assessment

This unit is assessed by an external examination set and marked by AQA. The examination takes place under controlled examination conditions and the exam date will be published at the start of each academic year.

Learners are allowed to use a non-programmable scientific calculator in the examination.

The examination consists of a written paper with two sections, A and B. Learners have to complete both sections and there are no optional questions within either section.

The examination is 2 hours duration and the total number of marks available in the examination is 80.

Section A is worth 50 marks and consists of relatively short questions based on the whole of the specification for this unit. Learners are required to answer all of the questions in Section A.
Section B is worth 30 marks and includes longer questions worth up to 15 marks each. The questions in Section B do not necessarily cover the whole of the specification for this unit at each assessment. Learners are required to answer all of the questions in Section B.

**Employer engagement guidance**

The organisation, its staff and learners must have access to employers and expertise. The organisation will have computer/technical staff who will understand the practical activities identified in the assessment outcomes. Local employers could be invited to discuss the skills and knowledge they require to support their IT systems, to inform the structure and specific hardware and software identified in the unit.

Employers may also be able to provide opportunities to visit IT facilities or provide placement or shadowing opportunities for assessors and/or learners to provide updating of the former and learning opportunities for the latter.

Employers could be invited to an apprenticeship forum.

The British Computer Society (BCS) and the Association of Computing Machinery are two examples of professional bodies who engage with learners.

**Delivery guidance**

Although, for the purposes of identifying specific assessment outcomes, areas such as hardware, software, networks etc, have been split into different elements of a computer system, it is not necessary or advisable to deliver the unit in this way.

Hardware and software could be taught together for example:

The CPU, for example, only understands ‘0’s and ‘1’s because at this level all instructions merely change the status of switches ‘off’ and ‘on’. Early programmers and some of those at the forefront of microchip technology still need to understand how to change the status to produce specific results and thus they need to understand binary arithmetic and machine code. Others, work at the next level of instructions where individual codes have been assembled into simple human instructions eg ‘load’, ‘execute’, where the assembler then breaks the instructions down into machine code for the computer to understand. From here the learner can go on to consider need for devices such as input and output devices and the role of the operating system and device drivers in enabling the CPU to carryout instructions. Once these are in place then the introduction of applications software becomes a requirement for those individuals who wish to use the capabilities of the computer rather than program each instruction for themselves. Practical skills can be incorporated by the learners discussing the need for devices such as graphics cards, printers, iris scanners and then identifying and installing the appropriate range of hardware; selecting the correct drivers and testing the installation. Finally, the applications software could be selected to operate the hardware and installed and tested in its turn. This could all take place as part of a scenario for designing a new computer system.

**Assessment outcome 1**

It is important that learners understand that computers are not limited to laptops or tablets but that they could be faced with larger and more complex machines.

The learner should have the opportunity to **research** the different computer types and **identify** the appropriate uses for each type.

This could include small group research and presentations of findings to the larger group, visits to local organisations with larger computer systems or presentations by individuals who work with the different computer types.
As a result the learners should be able to **explain** the advantages and disadvantages of a particular computer type in a given situation ie research, data warehousing, data mining, administration.

**Assessment outcome 2**

These are the physical components of the computer system and can be interpreted as anything that can be touched or felt. There have been many changes to computer hardware over time and new hardware and hardware modifications are appearing all of the time. Therefore, specific examples are intended only for guidance and should be adjusted to reflect the range of hardware available at the time of delivery and assessment of the unit. Learners should be able to **explore** the most up-to-date hardware available and **analyse** their strengths and weakness in order to **illustrate** their choice of hardware in a given scenario.

Where possible, learners should have the opportunity to identify components from computers using different CPU chips and operating systems and have access to either server-based systems or those who maintain such systems eg the organisation’s network and server technicians, who can explain how the hardware supports organisational requirements. It would be advantageous for learners to have physical access through opportunities to look at the inside of a computer. It is not necessary for learners to actually dismantle the computer themselves, but seeing the hardware in place does assist understanding of how buses, for example, link the various items together and what the components look like when properly installed.

Some components are separate identifiable parts, such as the motherboard or ports, whereas others such as the central processing unit (CPU), which in the case of personal computers (PCs) and servers, for example, normally contain the arithmetic logic unit (ALU), the control unit (CU) and small, fast registers of read/write memory within a single unit or ‘chip’. Learners should engage in class discussions or small group research activities to identify the individual components and their role in carrying out instructions and requests.

As the various parts are identified, a class or group discussion could take place as to the purpose, communication methods and location of each one. From this individuals or groups could create annotated diagrams of their findings, which could be discussed within the larger group or class.

For example, the learner would clearly benefit from being able to see and discuss as many of the following example devices as possible:

- input devices eg mouse, scanner, keyboard, touch screen, web cam, microphone, barcode reader, sensors
- external output devices eg printers (2D, 3D), screens, speakers, slide projectors
- secondary/backing storage eg hard disk drives, USB drives, read/writeable DVDs, removable magnetic disks, fixed magnetic disks, solid state drives (SSD).

**Assessment outcome 3**

These are the components of the computer system and can be interpreted as anything that cannot be touched, but ensures that the computer carries out the required task quickly and accurately. There have been many changes to computer software over time and new software is always becoming available. Therefore, specific examples are intended only for guidance and should be adjusted to reflect the range of software available at the time of delivery and assessment of the unit.

Learners could be provided with a computer system for which they would need to identify the appropriate operating systems, drivers, applications software etc. They could carry this out as a group or individually feeding back to the group through presentation, video or report.

The learners could carry out a theoretical activity where they would identify the necessary software for a written computer specification.
Presentations or sessions led by software or systems technicians would be beneficial to learners as the presenters could relate the software choices to actual events and possible issues which have arisen in the work place. This would assist learners in understanding the importance of software selection in the real world.

Learners should be able to explore the most up-to-date software available and analyse their strengths and weaknesses in order to illustrate their choice of hardware in a given scenario, through class discussion or small group research that could be fed back to the larger group.

Learners should consider different types of file storage and understand their purposes.

They could also work in pairs or small groups to investigate and provide feedback on specific types of security software such as antivirus, anti-spam and anti-malware, demonstrating a real understanding of the differences between these, and identifying examples of commonly used software to provide this functionality.

**Assessment outcome 4**

Learners could carry out individual research and then have a class discussion on the difference between information and data or a research project by small groups, who could report back their findings to the larger group for discussion through presentations or poster presentations, for example. Learners could be presented with information that has been broken down in to its component data items – eg lists of dates, names, places, images – and be asked to consider how they could be organised to provide information.

The difference between qualitative and quantitative data could be discussed by the class reviewing examples of both, eg feelings, colours, preferences (qualitative) and election results, annual rainfall, age profiles (quantitative).

It is also important that learners recognise that information must be checked to see that it is accurate, valid, timely and objective. The learners could be given examples of good and poor information and instructed to consider whether they meet the criteria and provide their reasoning. Online tutorials are also available to assist understanding of the characteristics of information. Learners could produce leaflets, booklets or electronic resources after carrying out their own investigations in small groups or individually.

Learners could be given examples of data and consider the processing required to convert them into useful information. The steps that they take could be used as the basis of a class discussion of the data processing cycle. They could identify the input data and the range of operations (both arithmetic and logical) that they carried out on the data; the final output could then be drawn together as a set of instructions or diagrammatic representation of the cycle.

**Assessment outcome 5**

Concepts such as character encoding and assembly language often involve numbers systems such as binary and hex, eg ASCII characters encoded in binary, performing arithmetic of hexadecimal values in assembly language etc. Learners should be able to accurately manipulate the various number systems eg addition, subtraction, conversions as well as understand the relationships between the machine code level and the complex higher level languages written from a human rather than a machine perspective. This will include the ability to evaluate different character encoding systems in terms of range of characters available, for example.

It is important that learners undertake practical exercises on number conversion, from one base to another, and practice arithmetic calculations; these must include denary, binary and hexadecimal bases and fractions. It may be possible to integrate this element of the assessment outcome with maths lessons or enable learners to develop presentations on number bases for other learners.
The same discussions could include the reasons for binary and hexadecimal being essential to computer instructions, linking it to bits, bytes, nibbles and words. From this, the matching of binary or hexadecimal numbers to human understandable characters could be discussed and small group research conducted into the reasons for the development of different character codes such as ASCII, Unicode and Extended Binary Coded Decimal Interchange Code (EBCDIC) and how they differ from each other.

The learners could research the different types of programming language and produce a diagram of their position on a line from machine understandable to human understandable formats. The programs must include machine code, assemblers, high level and 4GLs. The outcomes could then be discussed in terms of the ways in which different programs can be translated in to machine code.

Useful links and resources

Books


Websites

- [e-booksdirectory.com](http://e-booksdirectory.com) (online books for download or reading, some free resources).
### 12.2 Unit 2: Communication technologies

<table>
<thead>
<tr>
<th>Title</th>
<th>Communication technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>H/507/6426</td>
</tr>
<tr>
<td>Assessment</td>
<td>Externally assessed</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s)</td>
<td>N/A</td>
</tr>
<tr>
<td>contextualised within</td>
<td></td>
</tr>
<tr>
<td>this unit</td>
<td></td>
</tr>
</tbody>
</table>

**Resources required for this unit**

Suitable Windows PC, Linux, Apple Macintosh OS X, Apple iOS or other suitable platforms, that offer basic terminal utilities for connecting to networking devices such as firewalls, routers and switches. Most terminal utilities are either intrinsic to the operating system (eg Linux) or free to download (eg PuTTY, an Open Source certificate program). Point-to-point communication between two computer systems can also be attempted using similar software. This will, of course, also require the possession of suitable serial, parallel and/or network cables. Other utilities such as protocol analysers (eg Wireshark) are also useful to demonstrate network traffic and its protocols and data.

Wired and wireless networks should also be demonstrated and investigated. This will require a different selection of hardware and software, eg wireless access points (WAP), wireless routers, wireless network cards etc.

Learners should also have access to suitable offline and online learning material, manuals, help sheets and coded examples in order to encourage self-sufficiency.

**Synoptic assessment within this unit**

IT: Cyber Security linked to Units 1 and 3.

IT: Cyber Security and Security Administration linked to Units 1, 3 and 5.

This unit provides complementary coverage to Unit 1, Fundamental principles of computing, by moving the learner beyond a single ‘standalone’ computer system.

Unit 3 develops data communication concepts introduced in this unit by examining different types of networks, their logical and physical design, uses, basic security and implementation.

Unit 5 provides learners with an understanding of different numbers systems, many of which have key uses in different communication technologies.

A signposted breakdown can be found in this unit’s synoptic assessment guidance.

### Aim and purpose

This unit will provide the learner with the necessary knowledge to appreciate the fundamental aspects of data communication. It will enable a firm conceptual grasp of how data is transmitted at lightning speeds from one point to another, thereby enabling the modern technologies, devices and services we take for granted every single day.
Unit introduction

Communication technologies come in many shapes and sizes. In computing, the phrase is often used as an umbrella title to encapsulate a number of different technologies that we use each day, from the mobile telephone in our hand to the wireless network we have in our home or workplace.

In this unit, learners will gain an understanding of how devices communicate, focusing on both the physical transmission methods and the media that they use. An introduction to mobile technologies and networking is also provided, helping the learner to appreciate the range, variety and complexities of the hardware, software and services that are involved. By the unit’s completion, learners will have honed their practical skills in order to create basic wired and wireless communications using a variety of devices, media and techniques.

Unit content

Fundamentals of data communication

| Types of signal       | • Digital vs analogue signals; modulation.  
|                      | • Representing data electronically (bits, bytes, protocol data units, etc). |

| Type of terminal equipment | • Data terminal equipment (DTE).  
|                            | • Data circuit-terminating equipment (DCE). |

| Transmission types       | • Synchronous transmission of data.  
|                         | • Asynchronous transmission of data.  
|                         | • Packet vs circuit switching. |

| Error detection and correction | • Cause of errors, eg signal disruption through channel noise (crosstalk, interference, impulse), coupled noise, (industrial, atmospheric).  
|                               | • Error detection and correction techniques:  
|                               | • repetition codes  
|                               | • parity bits (odd, even)  
|                               | • checksum  
|                               | • cyclic redundancy checks (crcs). |

| Bandwidth               | • Bandwidth measurements, eg bit/s, kbit/s, Mbit/s, Gbit/s.  
|                        | • Typical speeds, eg Ethernet 10 Mbit/s, Fast Ethernet 100 Mbit/s, Gigabit Ethernet 1 Gbit/s.  
|                        | • Bandwidth limitation and noise.  
|                        | • Bandwidth as consumption: throttling, capping and allocation. |

Data communication methods

| Communication methods | • Point-to-point system, protocol and handshakes.  
|                      | • Basic communication types:  
|                      | • simplex  
|                      | • half-duplex  
|                      | • duplex.  
|                      | • Real world examples of the different communication types.  
|                      | • Serial and parallel communication, speeds and typical uses. |
## Data communication methods

### Transmission media

- **Wired:**
  - coaxial, unshielded and shielded twisted pair (UTP/STP).
  - Optical.
- **Wireless:**
  - infrared
  - radio
  - microwave
  - satellite.

### Transmission media features

- Reliability.
- Flexibility.
- Susceptibility to signal noise.
- Ease of installation.
- Effective operational range.
- Security.

## Basic mobile technology communication methods

### Fundamental concepts

- Mobile device; construction, components, etc.
- International mobile equipment identity (IMEI).
- Cells, base stations, roaming.
- Subscriber Identity Module (SIM), typical data stored in a SIM, eg International Mobile Subscriber Identity (IMSI), passwords, personal identification number (PIN), personal unblocking key (PUK).
- SIM form factors, eg mini-SIMs, micro-SIMs and nano-SIM.

### Mobile standards

- Standards and key features of:
  - Global System for Mobile (GSM)/2G
  - General Packet Radio Service (GPRS)/2.5G
  - Third Generation/3G
  - Fourth Generation/4G.
  - Licensed vs unlicensed technologies; frequencies, interference, strategies eg frequency hopping.

### Mobile services

- Short Message Service (SMS).
- Over-the-air (OTA) programming.
- Global Positioning System (GPS).
- Mobile broadband and tethering.

## The fundamentals of computer networks

### Network types

- Types and features of different types of computer network:
  - personal area network (PAN)
  - local area network (LAN)
  - wireless local area network (WLAN)
  - metropolitan area network (MAN)
  - wide area network (WAN)
  - storage area network (SAN).
The fundamentals of computer networks

<table>
<thead>
<tr>
<th>Network topologies</th>
<th>• Different topologies, their key features, strengths and weaknesses:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• bus</td>
</tr>
<tr>
<td></td>
<td>• ring</td>
</tr>
<tr>
<td></td>
<td>• star</td>
</tr>
<tr>
<td></td>
<td>• tree</td>
</tr>
<tr>
<td></td>
<td>• mesh</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network rewards</th>
<th>• Typical arguments for networking:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• sharing resources:</td>
</tr>
<tr>
<td></td>
<td>• data</td>
</tr>
<tr>
<td></td>
<td>• devices, eg printers</td>
</tr>
<tr>
<td></td>
<td>• applications</td>
</tr>
<tr>
<td></td>
<td>• internet and world wide web access</td>
</tr>
<tr>
<td></td>
<td>• improved communication:</td>
</tr>
<tr>
<td></td>
<td>• email</td>
</tr>
<tr>
<td></td>
<td>• instant message</td>
</tr>
<tr>
<td></td>
<td>• video conferencing</td>
</tr>
<tr>
<td></td>
<td>• intranet</td>
</tr>
<tr>
<td></td>
<td>• improved data security, eg less risk of data loss, central management of user rights and privileges</td>
</tr>
<tr>
<td></td>
<td>• enables remote working</td>
</tr>
<tr>
<td></td>
<td>• reduced costs, efficiency saving</td>
</tr>
<tr>
<td></td>
<td>• improved hardware and service monitoring.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network risks</th>
<th>• Hacking and disruption.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Loss of data.</td>
</tr>
<tr>
<td></td>
<td>• Loss of service.</td>
</tr>
<tr>
<td></td>
<td>• Loss of income.</td>
</tr>
<tr>
<td></td>
<td>• Compromise of data integrity.</td>
</tr>
<tr>
<td></td>
<td>• Loss of reputation; commercial damage.</td>
</tr>
</tbody>
</table>

Network conceptual models, protocols and devices

<table>
<thead>
<tr>
<th>The need for network models</th>
<th>• To abstract complex physical devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• To encourage interoperability between different equipment manufacturers.</td>
</tr>
<tr>
<td></td>
<td>• To standardise subject terminology.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Open systems interconnection (OSI) model</th>
<th>Seven Layer model:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Layer 1 Physical hardware eg signalling, wiring.</td>
</tr>
<tr>
<td></td>
<td>• Layer 2 Data links eg frames, packets.</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 Network.</td>
</tr>
<tr>
<td></td>
<td>• Layer 4 Transport eg streams, segments.</td>
</tr>
<tr>
<td></td>
<td>• Layer 5 Session eg authentication, encryption.</td>
</tr>
<tr>
<td></td>
<td>• Layer 6 Presentation.</td>
</tr>
<tr>
<td></td>
<td>• Layer 7 Application.</td>
</tr>
</tbody>
</table>
Network conceptual models, protocols and devices

TCP/IP – Transmission control protocol / internet protocol

- TCP/IP Layers:
  - network interface (link layer)
  - internet
  - transport
  - application.

Devices operating across the layers

- Generally:
  - web and application servers
  - network hosts
  - network management stations (NMSs).
- Specifically:
  - physical layer devices including:
    - network interface cards (NICs)
    - repeaters
    - hubs
  - network layer protocols and devices including:
    - internet protocols (IP) eg IPv6
    - routing information protocol (RIP)
    - open shortest path first (OSPF)
    - router
  - transport layer protocols:
    - transport control protocol (TCP)
    - user datagram protocols (UDP)
  - data link layer protocols including:
    - media access control (MAC)
    - IEEE 802 Standards eg
      - 802.4 Token passing bus
      - 802.5 Token passing ring
      - 802.7 Broadband LAN
      - 802.8 Fibre-optic LAN/MAN
      - 802.11 Wireless LAN.

Assessment outcomes

Learners will be able to:

Assessment outcome 1: Understand the fundamentals of data communication

- a Types of signal, modulation, transmission type and terminal equipment.
- b Methods of representing and measuring data electronically.
- c The principles of noise, error detection and correction techniques.
- d Bandwidth allocation, limitation and management.
Assessment outcome 2: Analyse data communication methods

a  Communication methods and speeds in real world situations.
b  The application of wired and wireless transmission media.
c  The physical and abstract features of transmission media.

Assessment outcome 3: Analyse basic mobile technology communication

a  Mobile device components, including SIMs.
b  How mobile devices connect to, and are identified on, a local and international network.
c  The evolution of subscriber identification modules and mobile telecommunications technology.
d  Licensed and unlicensed technologies and strategies for dealing with interference.
e  Mobile services including SMS, OTA, GPS, mobile broadband and tethering.

Assessment outcome 4: Understand the fundamentals of computer networks

a  Types and features of different area networks.
b  The arrangement of the various elements of a computer network.
c  The rewards of networking vs the practical, commercial and individual risks.

Assessment outcome 5: Understand network conceptual models, protocols and devices

a  Network models and the need for standardisation.
b  The functions of, and the relationship between, the abstraction layers of the OSI conceptual models and internet protocol (IP) suite.
c  The functionality of devices operating across the layers and explain the protocols.

Assessment

This unit is assessed by an external examination set and marked by AQA. The examination takes place under controlled examination conditions and the exam date will be published at the start of each academic year.

Learners are allowed to use a non-programmable scientific calculator in the examination.

The examination consists of a written paper with two sections, A and B. Learners have to complete both sections and there are no optional questions within either section.

The examination is 2 hours duration and the total number of marks available in the examination is 80.

Section A is worth 50 marks and consists of relatively short questions based on the whole of the specification for this unit. Learners are required to answer all of the questions in Section A.

Section B is worth 30 marks and includes longer questions worth up to 15 marks each. The questions in Section B do not necessarily cover the whole of the specification for this unit at each assessment. Learners are required to answer all of the questions in Section B.
Employer engagement guidance

The organisation, its staff and learners must have access to employers and expertise. The organisation will have computer/technical staff who will understand the practical activities identified in the assessment outcomes. Local employers could be invited to discuss the skills and knowledge they require to support their IT systems, to inform the structure and specific hardware and software identified in the unit.

Employers may also be able to provide opportunities to visit IT facilities or provide placement or shadowing opportunities for assessors and/or learners to provide updating of the former and learning opportunities for the latter.

Employers could be invited to an apprenticeship forum.

The British Computer Society (BCS) and the Association of Computing Machinery are two examples of professional bodies who engage with learners.

Delivery guidance

It is recommended that this unit is taught as a precursor to Unit 3: Developing and maintaining computer networks, as many of its concepts are introduced in this unit.

Although it is suggested that the content is delivered to follow the order of the learning outcomes in this unit specification, it is not the only sequence that could be used. Tutors are encouraged to consider the holistic nature of the learner’s programme and the scheme itself.

Learners must have access to the hardware and software facilities necessary for the opportunity to generate evidence of all of the grading criteria listed. In the case of mobile communications technology it is perfectly possible that a learner’s device may be used if they accept the risks associated with connecting to potentially unsecured services and devices. As such, if centres cannot guarantee these resources, the unit should not be attempted.

Assessment outcome 1

Learners will develop and demonstrate their knowledge and understanding of data communication fundamentals. They should explore the difference between encoding data as digital and analogue signals. This is best achieved using simple diagrams or animations, further supported by demonstrating practical skills in encoding sample data, comparing and contrasting the different causes of error that could disrupt the signal and finally including an error detection method to identify the problem.

Learners should be able to calculate data transfer times depending on available bandwidth. They must use the correct units and interpret the metrics correctly in order to calculate sensible answers. Comparisons can be made with many online ‘broadband speed tests’ that perform similar tasks in an automated fashion. Complications arise when bandwidth is constrained in some fashion and learners should understand these impacts, especially in terms of potential impact on speed and sustained connectivity.

Assessment outcome 2

This focuses on the learner being able to demonstrate the range of their knowledge of different communication methods and media. These essentially involve the learner performing the necessary practical tasks and then documenting to a satisfactory standard to ensure that they have an embedded understanding of the concepts. As part of their development they could, for example, make data connections between two devices, potentially a DTE and a DCE or two DTEs using either a parallel or serial cable. They should be able to demonstrate an understanding of the different communication types and protocols that could be used in a point-to-point system. Exploring real world connectivity issues and being able to justify the communication type and protocol that would be most effective would be a way to show their understanding.
Learners should be able to understand wired and wireless transmission media, and should practically complete both a suitable wired and wireless connection, then determine which method would be most suited to a selected real world situation or case study. This type of task can be completed through a combination of practical activity, maybe presenting their findings to the group.

**Assessment outcome 3**

This outcome revolves around the use of mobile technology and learners have an opportunity to study their own resources. Learners should be able to demonstrate a working knowledge of the components of a mobile device: they should be able to provide technical descriptions rather than a superficial overview of the device. They should be able to explain the device in terms of its cellular infrastructure, explaining how data (eg voice, SMS text messages etc) is transferred from device to device. Learners should practice the evaluation of the features and functionality that specific services provide.

An investigation into the key features of mobile standards and the services offered through devices could be achieved through pair or group work; creating an information leaflet, presentation or booklet would help them to understand the differences.

**Assessment outcome 4**

In this outcome, learners need to explore the basic concepts of different network types and their topologies. They should be able to identify the different types of network and topologies, linking this to real world examples. The centre’s own network will provide an opportunity for exploration.

Learners should gain sufficient technical knowledge to enable them to create a rationale for the choice of particular technologies for installing a network and they should be able to articulate the risks that the business could face. The key to this outcome is that learners should be able to make reasoned judgements about the recommendations they make in context.

**Assessment outcome 5**

This outcome focuses on the mapping of conceptual models to real life hardware and software that are used in a networked solution. Learners should be able to chart data travelling through the different layers of a conceptual model. This is most easily achieved pictorially, either through a static chart or diagram, or through a simple slideshow or animation. Learners could undertake pair or small group work against a variety of scenarios, being able to compare and contrast two different conceptual models.

To complete the unit learners should demonstrate their understanding by correctly using different networking devices (three would be recommended) at different conceptual levels and generating evidence to demonstrate the correct network protocols that might operate at different layers. This could be best achieved through the use of a protocol analyser.

**Synoptic assessment guidance**

Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.
A01: Understand the fundamentals of data communication

This assessment outcome introduces the basic concepts of data communication including the types of signal, terminal, transmission types, error detection and bandwidth. Many units develop these concepts and provide practical examples of their use, features and functions.

Unit 1 – AO5: Demonstrate how computers process user requirements
This unit’s assessment outcome, typically taught in parallel, supports the learners’ understanding of bandwidth measurements by introducing the various units used in computing (eg Megabits, Gigabits etc. The learner should benefit from seeing these units in a practical context.

Unit 3 – PO2: Identify the different types of network architectures and technology types
Unit 3’s second performance outcome enhances the learners’ understanding of circuit and packet switching, LAN Technologies and WAN technologies.

Unit 5 – PO1: Work with number systems
Many concepts connected with low level data communication, eg digital signals, parity bits etc rely on the learners’ appreciation of other number systems, particularly binary. This unit’s first performance outcome provides a firm grounding of the various number systems used in computing.

A02: Analyse data communication methods

This assessment outcome examines the different methods used to communicate data, the media used and their attendant features.

Unit 1 – AO2: Understand the hardware components of a computer system
Learners may be able to analyse data communication methods more ably through their introduction to the recognisable serial and parallel communication methods studied in this unit.

Unit 3 – PO2: Identify the different types of network architectures and technology types
Transmission media and their features are explored in more detail through this performance outcome. Practical emphasis placed on LAN technologies, different transmission methods and media, eg wired (copper, optical) and wireless and their connectors should reinforce the learners’ recognition factor.

A03: Analyse basic mobile technology communication

This assessment outcome focuses on mobile technologies; the hardware used, its organisation, current standards and available services.

Unit 1 – AO1: Identify the different types of computer
Learners access this type of communication technology through various mobile devices (eg tablets etc), many of which may be introduced as a type of personal computer in this assessment outcome. Learners should benefit from being able to connect the tangible hardware with the more conceptual ideas involved in mobile communication.
AO4: Understand the fundamentals of computer networks
This assessment outcome introduces the idea of a network by examining the different sizes available, their relevant topologies and the balance of risk and reward that a network may provide.

Unit 3 – PO1: Identify communication activities facilitated by computer networks
This performance outcome provides extended topic coverage for network rewards, eg personal communication, business and e-business applications, that the learner may find helpful when attempting to explain the attractions of a network.

Unit 3 – PO2: Identify the different types of network architectures and technology types LAN, WAN, WLAN etc

Unit 3 – PO3: Understand the different types of local area networks (LANs) and wide area networks (WANs)
These performance outcomes help the learner to explore the practical creation of LANs and WANs. In doing so, learners should have a better understanding of their similarities and differences.

AO5: Evaluate network conceptual models, protocols and devices
This assessment outcome asks learners to evaluate the different models, protocols and devices that are used to describe network systems in a logical manner.

Unit 1 – PO2: Understand the hardware requirements of a computer system
This assessment outcome introduces the concept of expansion cards. One of these, the network interface cards (NICs), should provide the learner with a perfect example of a device operating at the physical layer.

Unit 3 – PO2: Identify the different types of network architectures and technology types
This unit’s second performance outcome provides coverage of many data link layer protocols and standards, eg the Institute of Electrical and Electronics Engineers (IEEE) 802 family for LAN, WLAN (wireless LAN) etc.

Useful links and resources

Books

Websites
• Serial Communication: learn.sparkfun.com/tutorials/serial-communication/rules-of-serial
• Search Mobile Computing: searchmobilecomputing.techtarget.com
• Cisco: cisco.com
• The OSI Model’s Seven Layers: support.microsoft.com/kb/103884
• Wireshark Protocol Analyser: wireshark.org/download.html
• PuTTY: chiark.greenend.org.uk/~sgtatham/putty/download.html
### 12.3 Unit 3: Developing and maintaining computer networks

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Developing and maintaining computer networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit number</strong></td>
<td>K/507/6427</td>
</tr>
<tr>
<td><strong>Unit assessment type</strong></td>
<td>Centre assessed and externally quality assured</td>
</tr>
<tr>
<td><strong>Recommended assessment method</strong></td>
<td>Practical assignment</td>
</tr>
<tr>
<td></td>
<td>This is the preferred assessment method for this unit. A centre may choose an alternative method of assessment, but will be asked to justify as part of the quality assurance process.</td>
</tr>
<tr>
<td><strong>Guided learning hours</strong></td>
<td>90</td>
</tr>
<tr>
<td><strong>Transferable skill(s)</strong> contextually within this unit</td>
<td>Research⁴</td>
</tr>
<tr>
<td><strong>Resources required for this unit</strong></td>
<td>A live network environment.</td>
</tr>
<tr>
<td></td>
<td>Network hardware and software.</td>
</tr>
<tr>
<td></td>
<td>A range of tools including multi-meters, screw drivers, pliers, wire cutters, rubber matting and anti-static wrist bands, lifting and moving equipment.</td>
</tr>
<tr>
<td></td>
<td>Professional documentation for designing and maintaining networks (may be available from own institution).</td>
</tr>
<tr>
<td></td>
<td>A range of wiring, conduits, connectors, etc.</td>
</tr>
<tr>
<td><strong>Synoptic assessment within this unit</strong></td>
<td>IT: Cyber Security linked to Units 1 and 2.</td>
</tr>
<tr>
<td></td>
<td>IT: Cyber Security and Security Administration linked to Units 1, 2 and 5.</td>
</tr>
<tr>
<td></td>
<td>Draws on underlying principles of computer applications and data concepts discussed in Unit 1.</td>
</tr>
<tr>
<td></td>
<td>Unit 2 provides the learner with the underlying principles of data communication and the technologies used to build networks, introducing many of the building blocks of any networked solution.</td>
</tr>
<tr>
<td></td>
<td>Investigations into network performance levels and faults may provide fascinating data sets that can be used to exercise numeracy skills such as calculating probability, and gathering and interpreting data – both core aspects of Unit 5.</td>
</tr>
<tr>
<td></td>
<td>Any networking design and planning will also thematically embrace security concepts drawn from Units 4, 6 and 7, particularly in terms of meeting ongoing maintenance challenges and protecting the network from emerging threats and vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>A signposted breakdown can be found in this unit’s synoptic assessment guidance.</td>
</tr>
</tbody>
</table>

⁴ Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.
Aim and purpose
This unit will provide learners with the underpinning knowledge and understanding of a range of computer networks and methodologies to enable them to develop a simple network from a specification and also the practical skills required to be able to develop and maintain networks for an organisation.

Unit introduction
Computers, except those used for specific security sensitive purposes, are almost invariably linked to other computers through at least one network and often more than one. The development and maintenance of networks is therefore essential to modern business and everyday life.

Being online, linked to other machines, is essential for work, engaging with health, taxation, or other public bodies, and entertainment.

Even in small businesses or in the home, computers, mobile telephones and tablets are linked to each other, the television and one or more printers. Thus the ability to understand the types of network available, their strengths and weaknesses, the purpose of the components required and being able to build and maintain a network is valuable for anyone who works with computers.

Learners studying this unit would benefit from having initially studied Unit 2: Communication technologies.

This unit provides an opportunity to evidence achievement of the transferable skill of research.

Unit content

<table>
<thead>
<tr>
<th>Communication activities facilitated by computer networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of personal communication using a computer</td>
</tr>
<tr>
<td>(eg)</td>
</tr>
<tr>
<td>• Blog.</td>
</tr>
<tr>
<td>• Instagram.</td>
</tr>
<tr>
<td>• Podcasts.</td>
</tr>
<tr>
<td>• Email.</td>
</tr>
<tr>
<td>• Wikis.</td>
</tr>
<tr>
<td>• Social networks.</td>
</tr>
<tr>
<td>Business applications</td>
</tr>
<tr>
<td>(eg)</td>
</tr>
<tr>
<td>• Project management.</td>
</tr>
<tr>
<td>• Diaries.</td>
</tr>
<tr>
<td>• Meeting planners.</td>
</tr>
<tr>
<td>• Spreadsheets.</td>
</tr>
<tr>
<td>• Databases.</td>
</tr>
<tr>
<td>• Documents.</td>
</tr>
<tr>
<td>E-Business applications</td>
</tr>
<tr>
<td>(eg)</td>
</tr>
<tr>
<td>• Banking.</td>
</tr>
<tr>
<td>• Retail.</td>
</tr>
<tr>
<td>• Marketing.</td>
</tr>
<tr>
<td>• Finance.</td>
</tr>
</tbody>
</table>
### Types of network architectures and technology types

<table>
<thead>
<tr>
<th>Network architectures</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Peer-to-peer.</td>
<td></td>
</tr>
<tr>
<td>• Client/server.</td>
<td></td>
</tr>
<tr>
<td>• Virtual Local Area Network (VLAN).</td>
<td></td>
</tr>
<tr>
<td>• Virtual Private Networks (VPN).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local area network (LAN) technologies and properties</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Types eg:</td>
<td></td>
</tr>
<tr>
<td>• Ethernet; Institute of Electrical and Electronics Engineers (IEEE 802.3)</td>
<td></td>
</tr>
<tr>
<td>• 10Base-T (IEEE 802.3i)</td>
<td></td>
</tr>
<tr>
<td>• 100Base-TX (IEEE 802.3u)</td>
<td></td>
</tr>
<tr>
<td>• 10GBase-T (IEEE 802.3an)</td>
<td></td>
</tr>
<tr>
<td>• Properties:</td>
<td></td>
</tr>
<tr>
<td>• transmission media:</td>
<td></td>
</tr>
<tr>
<td>• copper wire (twisted pair)</td>
<td></td>
</tr>
<tr>
<td>• single mode optical fibre</td>
<td></td>
</tr>
<tr>
<td>• multi-mode optical fibre</td>
<td></td>
</tr>
<tr>
<td>• speed</td>
<td></td>
</tr>
<tr>
<td>• duplex</td>
<td></td>
</tr>
<tr>
<td>• distance</td>
<td></td>
</tr>
<tr>
<td>• carrier sense multiple access with collision detection (CSMA/CD)</td>
<td></td>
</tr>
<tr>
<td>• broadcast</td>
<td></td>
</tr>
<tr>
<td>• collision</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless local area networks (WLAN) technologies and properties</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Types:</td>
<td></td>
</tr>
<tr>
<td>• wi-fi 802.11</td>
<td></td>
</tr>
<tr>
<td>• bluetooth</td>
<td></td>
</tr>
<tr>
<td>• Properties:</td>
<td></td>
</tr>
<tr>
<td>• 802.11 IEEE standards, eg 802.11b, 802.11g, 802.11n</td>
<td></td>
</tr>
<tr>
<td>• frequency, eg 2.4 ghz and 5 ghz</td>
<td></td>
</tr>
<tr>
<td>• speed</td>
<td></td>
</tr>
<tr>
<td>• distance</td>
<td></td>
</tr>
<tr>
<td>• interference</td>
<td></td>
</tr>
</tbody>
</table>
## Types of network architectures and technology types

<table>
<thead>
<tr>
<th>Wide area network (WAN) technologies and properties</th>
<th>Types eg:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- frame relay</td>
</tr>
<tr>
<td></td>
<td>- Asynchronous Transfer Mode (ATM)</td>
</tr>
<tr>
<td></td>
<td>- Integrated Services Digital Network (ISDN)</td>
</tr>
<tr>
<td></td>
<td>- wireless</td>
</tr>
<tr>
<td></td>
<td>- Very High Bit Rate Digital Subscriber Line (VDSL).</td>
</tr>
<tr>
<td></td>
<td>Properties:</td>
</tr>
<tr>
<td></td>
<td>- speed</td>
</tr>
<tr>
<td></td>
<td>- distance</td>
</tr>
<tr>
<td></td>
<td>- transmission media</td>
</tr>
<tr>
<td></td>
<td>- circuit switch</td>
</tr>
<tr>
<td></td>
<td>- packet switch.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wiring standards</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Coaxial.</td>
</tr>
<tr>
<td></td>
<td>- Category 5 and 6 Unshielded Twisted Pair (UTP).</td>
</tr>
<tr>
<td></td>
<td>- Fibre optic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network hardware</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- File servers.</td>
</tr>
<tr>
<td></td>
<td>- Proxy servers.</td>
</tr>
<tr>
<td></td>
<td>- Connection devices.</td>
</tr>
<tr>
<td></td>
<td>- Wireless devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connectors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- UTP:</td>
</tr>
<tr>
<td></td>
<td>- registered Jack –RJ connectors eg:</td>
</tr>
<tr>
<td></td>
<td>- RJ-45</td>
</tr>
<tr>
<td></td>
<td>- RJ-11.</td>
</tr>
<tr>
<td></td>
<td>- Optical Fibre connectors eg:</td>
</tr>
<tr>
<td></td>
<td>- straight tip (ST)</td>
</tr>
<tr>
<td></td>
<td>- subscriber connector (SC)</td>
</tr>
<tr>
<td></td>
<td>- mechanical transfer registered jack (MT-RJ)</td>
</tr>
<tr>
<td></td>
<td>- local connector (LC).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Media converters</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Single mode fibre to Ethernet.</td>
</tr>
<tr>
<td></td>
<td>- Fibre to coaxial.</td>
</tr>
<tr>
<td></td>
<td>- Single mode to multimode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cables</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Serial.</td>
</tr>
<tr>
<td></td>
<td>- RS 232.</td>
</tr>
<tr>
<td></td>
<td>- Universal Serial Hub.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cabling standards</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- 565A.</td>
</tr>
<tr>
<td></td>
<td>- 565B.</td>
</tr>
</tbody>
</table>
**Types of network architectures and technology types**

<table>
<thead>
<tr>
<th>Cable installation</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Main distribute frame.</td>
<td></td>
</tr>
<tr>
<td>• 25 pair.</td>
<td></td>
</tr>
<tr>
<td>• 110 block.</td>
<td></td>
</tr>
<tr>
<td>• Broadband over power.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network connecting devices</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• NIC.</td>
<td></td>
</tr>
<tr>
<td>• Hub.</td>
<td></td>
</tr>
<tr>
<td>• Switch.</td>
<td></td>
</tr>
<tr>
<td>• Basic bridge.</td>
<td></td>
</tr>
<tr>
<td>• Router.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network wireless devices</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Wireless access point (WAP).</td>
<td></td>
</tr>
<tr>
<td>• Wireless antennae:</td>
<td></td>
</tr>
<tr>
<td>• point-to-point (PPP)</td>
<td></td>
</tr>
<tr>
<td>• point-to-multi-point (PMP).</td>
<td></td>
</tr>
<tr>
<td>• Wireless ethernet bridge.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic network security</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• User accounts.</td>
<td></td>
</tr>
<tr>
<td>• User passwords.</td>
<td></td>
</tr>
<tr>
<td>• Access control lists (ACLs).</td>
<td></td>
</tr>
<tr>
<td>• Internet protocol (IP) address filtering.</td>
<td></td>
</tr>
<tr>
<td>• Media access control (MAC) filtering.</td>
<td></td>
</tr>
<tr>
<td>• Encryption methods, eg wired equivalent privacy (WEP), Wi-Fi protected access (WPA, WPA2) etc.</td>
<td></td>
</tr>
<tr>
<td>• Honeypots.</td>
<td></td>
</tr>
</tbody>
</table>

**Types of local area networks (LANs) and wide area networks (WANs)**

<table>
<thead>
<tr>
<th>Local area networks (LAN)</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personal area network (PAN).</td>
<td></td>
</tr>
<tr>
<td>• Enterprise area network (EAN).</td>
<td></td>
</tr>
<tr>
<td>• Campus area network (CAN).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wide area network (WAN)</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Joint academic network (JANET).</td>
<td></td>
</tr>
<tr>
<td>• Virtual private network (VPN).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other network types</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• System area network.</td>
<td></td>
</tr>
<tr>
<td>• Storage area network.</td>
<td></td>
</tr>
</tbody>
</table>
## Designing and building a network from a specification

### Planning

- Create outline document:
  - goals
  - business requirements
  - constraints, eg physical environment, cost, time etc
  - minimum performance requirements.
  - regulatory and legislative requirements:
    - internal:
      - organisational policies and procedures
    - external:
      - laws and statutes
      - regulations eg ISO/IE 27002
      - standards.
  - Wiring diagrams.
  - Network diagrams:
    - physical
    - logical
    - software tools.

### Build a network to meet the specification

- Select components eg wiring, connectors, hub, workstations.
- Select appropriate tools eg rubber mats, antistatic wrist bands, multi-meters, correct range of screwdrivers, wire cutters, wire strippers, crimpers etc.
- Follow health and safety and other related requirements:
  - Health and Safety at Work Act 1974
  - Health and Safety (Display Screen Equipment) Regulations 1992
  - Waste Electrical and Electronic Equipment recycling (WEEE) 2006
  - Manual Handling Operations Regulations 1992 (as amended)
  - Electricity at work: Safe working practices (HSE).

### End user network testing

#### Testing techniques

(eg)
- Simulation and replication.
- Substitution.
- Elimination.
- Upgrade, eg BIOS support (flashing), drivers.
- Reinstall software eg drivers or applications.
- Operating system support, updates and patches.

#### Benchmarking

- Benchmark metrics eg response time, throughput, packet drop, streaming, etc.
- Benchmarking software eg LAN/WAN speed tests, network stress tests, Quality of Service (QoS).
# End user network testing

<table>
<thead>
<tr>
<th>Diagnostic hardware tools</th>
<th>Tools eg:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multi-meter</td>
</tr>
<tr>
<td></td>
<td>network multi-meter</td>
</tr>
<tr>
<td></td>
<td>network cable testers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firmware self-diagnostic routines</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Power on Self-Test (POST).</td>
</tr>
<tr>
<td></td>
<td>Network Interface Card (NIC) tests.</td>
</tr>
<tr>
<td></td>
<td>Preboot Execution Environment (PXE) boot test.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Simple network management protocol (SNMP)</th>
<th>Components:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>managed device</td>
</tr>
<tr>
<td></td>
<td>agent</td>
</tr>
<tr>
<td></td>
<td>network management station (NMS).</td>
</tr>
<tr>
<td></td>
<td>Devices that support SNMP:</td>
</tr>
<tr>
<td></td>
<td>routers</td>
</tr>
<tr>
<td></td>
<td>switches</td>
</tr>
<tr>
<td></td>
<td>servers</td>
</tr>
<tr>
<td></td>
<td>workstations</td>
</tr>
<tr>
<td></td>
<td>printers.</td>
</tr>
<tr>
<td></td>
<td>Protocols.</td>
</tr>
<tr>
<td></td>
<td>Proxy agents.</td>
</tr>
<tr>
<td></td>
<td>Bilingual network-management systems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intrusion detection system (IDS)</th>
<th>Network intrusion detection system (NIDS).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Host intrusion detection system (HIDS).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firewall</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware, software, rules, exceptions, Stateful Packet Inspection (SPI) and application layer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diagnostic software tools</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Control panel (connections, adaptors).</td>
</tr>
<tr>
<td></td>
<td>Ping.</td>
</tr>
<tr>
<td></td>
<td>Traceroute.</td>
</tr>
<tr>
<td></td>
<td>IPconfig/IFconfig.</td>
</tr>
<tr>
<td></td>
<td>Netstat.</td>
</tr>
<tr>
<td></td>
<td>Nbstat.</td>
</tr>
<tr>
<td></td>
<td>Address resolution protocol (ARP).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Steps in trouble shooting</th>
<th>Identify problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gather information.</td>
</tr>
<tr>
<td></td>
<td>Question users.</td>
</tr>
<tr>
<td></td>
<td>Look for changes.</td>
</tr>
<tr>
<td></td>
<td>Identify possible issues.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error logs</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating system.</td>
</tr>
<tr>
<td></td>
<td>Network service (eg HTTP, FTP) and application.</td>
</tr>
</tbody>
</table>
## End user network testing

<table>
<thead>
<tr>
<th>Error codes and messages</th>
<th>• Different formats (eg hexadecimal, binary etc) eg generated via hardware, BIOS, operating system, applications and utilities etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>• Recording outcomes and recommendations.</td>
</tr>
<tr>
<td>Test plan</td>
<td>• Features to be tested.</td>
</tr>
<tr>
<td></td>
<td>• Features not to be tested.</td>
</tr>
<tr>
<td></td>
<td>• Approach eg testing level, testing types, testing methods.</td>
</tr>
<tr>
<td></td>
<td>• Pass/fail criteria.</td>
</tr>
<tr>
<td></td>
<td>• Test deliverables eg test plan, test cases, test scripts, defect logs, test reports.</td>
</tr>
<tr>
<td></td>
<td>• Test environment:</td>
</tr>
<tr>
<td></td>
<td>• hardware, software, network</td>
</tr>
<tr>
<td></td>
<td>• testing tools.</td>
</tr>
<tr>
<td></td>
<td>• Estimate of costs.</td>
</tr>
<tr>
<td></td>
<td>• Schedule ie key milestones.</td>
</tr>
<tr>
<td></td>
<td>• Responsibilities.</td>
</tr>
<tr>
<td></td>
<td>• Test results.</td>
</tr>
<tr>
<td></td>
<td>• Remedial steps taken.</td>
</tr>
<tr>
<td></td>
<td>• Sign off performance.</td>
</tr>
</tbody>
</table>

## Maintaining a network system

<table>
<thead>
<tr>
<th>Agree a service level agreement (SLA)</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• A description of the services to be provided and for whom.</td>
</tr>
<tr>
<td></td>
<td>• Roles, responsibilities of team members and contact details.</td>
</tr>
<tr>
<td></td>
<td>• Availability of the service.</td>
</tr>
<tr>
<td></td>
<td>• Service standards eg speed of reply to request.</td>
</tr>
<tr>
<td></td>
<td>• Customer responsibilities.</td>
</tr>
<tr>
<td></td>
<td>• Legal or other regulations that must be complied with.</td>
</tr>
<tr>
<td></td>
<td>• Qualitative and quantitative measures to monitor and evaluate service.</td>
</tr>
<tr>
<td></td>
<td>• Communication methods.</td>
</tr>
<tr>
<td></td>
<td>• Key performance indicators.</td>
</tr>
<tr>
<td></td>
<td>• How complaints will be dealt with.</td>
</tr>
<tr>
<td></td>
<td>• How the agreement will be reviewed and updated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complete network documentation</th>
<th>• Records of tests.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Records of installations and upgrades.</td>
</tr>
<tr>
<td></td>
<td>• Records of issues.</td>
</tr>
<tr>
<td></td>
<td>• Records of details of resolution of issues.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Carry out preventive maintenance</th>
<th>• Test network for weaknesses eg reduced speeds, loss of connections.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Installing upgrades and new hardware or software.</td>
</tr>
<tr>
<td></td>
<td>• Installing or upgrading security software.</td>
</tr>
<tr>
<td></td>
<td>• Monitoring traffic and bottlenecks.</td>
</tr>
</tbody>
</table>
### Performance outcomes

On successful completion of this unit learners will be able to:

<table>
<thead>
<tr>
<th>Performance outcome 1:</th>
<th>Identify communication activities facilitated by computer networks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance outcome 2:</td>
<td>Identify the different types of network architectures and technology types.</td>
</tr>
<tr>
<td>Performance outcome 3:</td>
<td>Understand different types of local area networks (LANs) and wide area networks (WANs).</td>
</tr>
<tr>
<td>Performance outcome 4:</td>
<td>Design and build a network from a specification.</td>
</tr>
<tr>
<td>Performance outcome 5:</td>
<td>Undertake end user network testing.</td>
</tr>
<tr>
<td>Performance outcome 6:</td>
<td>Maintain a network system.</td>
</tr>
</tbody>
</table>

### Grading criteria

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pass</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To achieve a pass the learner must evidence that they can:</td>
<td></td>
<td></td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
</tr>
<tr>
<td><strong>Merit</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO1: Identify communication activities facilitated by computer networks</strong></td>
<td><strong>P1</strong> Describe nine activities which are supported by networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO2: Identify the different types of network architectures and technology types</strong></td>
<td><strong>P2</strong> Describe four architectures.</td>
<td><strong>M1</strong> Develop a network architecture for a defined user need.</td>
<td><strong>D1</strong> Justify the choice of network architecture.</td>
</tr>
<tr>
<td><strong>P3</strong> Identify the network components for a defined user need.</td>
<td></td>
<td><strong>M2</strong> Explain the choice of components.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| PO3: Understand the different types of local area networks (LANs) and wide area networks (WANs) | <strong>P4</strong> Research and map different types of network technologies. | | |
| <strong>P5</strong> Using research describe the main characteristics and properties of two WAN and two LAN technologies. | | | |</p>
<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO4: Design and build a network from a specification</strong></td>
<td>To achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td><strong>P6</strong> Produce an outline planning document for defined user need.</td>
<td><strong>M3</strong> Produce diagrammatic representations of the network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P7</strong> Identify the components and the correct tools required to build the network defined.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P8</strong> Build the network defined.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P9</strong> Follow relevant health and safety regulations when building the network.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO5: Undertake end user network testing</strong></td>
<td><strong>P10</strong> Describe five testing techniques.</td>
<td><strong>M4</strong> Justify the importance of network benchmarking in system testing.</td>
<td></td>
</tr>
<tr>
<td><strong>P11</strong> Identify at least three network faults on a selected system.</td>
<td><strong>M5</strong> Justify the testing techniques to be used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P12</strong> Record fault information and create a test plan, identifying the appropriate tools and components required to carry out tests.</td>
<td><strong>M6</strong> Analyse the test results.</td>
<td><strong>D2</strong> Evaluate the testing process.</td>
<td></td>
</tr>
</tbody>
</table>
To achieve a pass the learner must evidence that they can:

In addition to the pass criteria, to achieve a merit the evidence must show the learner can:

In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO6: Maintain a network system</td>
<td>P14 Provide evidence of following the requirements of an SLA.</td>
<td>M7 Record and interpret information from complete network documentation.</td>
<td>D3 Demonstrate preventive maintenance activities in meeting all requirements of the SLA.</td>
</tr>
</tbody>
</table>

**Assessment amplification**

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

In completing performance criteria P4 and P5, learners will be presented with an opportunity to demonstrate the transferable skill of research.

Learners could use scenarios that cover a range of all of the performance outcomes. If the learners have the opportunity to have a work placement or a job in network support then they may be able to use evidence from these activities for some or all of the performance criteria.

For P1 learners could produce a presentation or report on ways in which networks support at least nine different activities, clearly linking application to the value of having a network link.

For M1 learners identify a preferred architecture and produce a design that would meet the needs of the scenario.

For P3 learners could produce a table, an annotated list or report.

P4 and P5 are research-based and could be evidenced together as a presentation with detailed handouts or a report. Learners could make an educational video clip or animation that explores the context in which different types of LAN and WAN are used and then describe the main characteristics that differentiate them.

For P6 learners will work on a scenario (preferably an employer brief) to produce an outline planning document for a network. This should include information about the user requirements, chosen architecture, components etc. The inclusion of diagrammatic representations to enhance the planning document and provide a visual overview of the system will provide evidence for M3.

For P9 learners should be observed throughout as they will need to demonstrate that they can work safely.

For P11 the evidence could be faults arising during the building of the network in PO4 or faults on another network. The evidence could be a fault log.

For P14 evidence could be presented as a log of activities linked to an agreed SLA signed off by their manager or tutor confirming that the activities have taken place and the SLA has been met.
Employer engagement guidance
The institution could engage with local employers and their own network staff to provide staff to
discussion networks with learners and provide work based opportunities or cases, scenarios and
projects that learners could use for training and assessment purposes.

The British Computer Society (BCS) and the European arm of the Association for Computing Machinery,
for example, may be willing to engage with learners in discussions on networking.

Delivery guidance

General comment
Learners studying this module would benefit from having studied Unit 2 Communication technologies.

The assessment criteria could be delivered holistically rather than as discrete elements through project
work or work placement opportunities.

It would be very useful if learners could engage in work placement activities for this unit, if this is not
possible then the learner must have access to a network development or training facility in order to
carry out the design, building and testing activities that are essential elements of this unit.

Performance outcome 1
The learners could carry out research in small groups, class discussions or visits to, or discussions with,
network specialists within the organisation or with external institutions.

Performance outcome 2
The learners could investigate a range of networks such as those within the institution, local
organisation, or their own home networks and feed this back to the group in order to consolidate an
agreed understanding of the topologies. From these discussions the learners could, as a group, identify
the logical topology for each physical network they have identified.

The class could research the types of technology and their properties through further investigation into
topologies and in discussion, if possible, with staff who support or manage the networks. However, if
this is not possible then a class brain storming session could be used.

All of the unit content should be covered, but it is not expected that the learners would have
encountered all of the elements in their investigations into specific topologies.

Performance outcome 3
Either individually or in small groups, learners could carry out an investigation into different types
of LANs and WANs. The investigations could take the form of online research, surveys of local
organisations and discussions with network professionals. The results could then be presented to
the wider group and a discussion take place as to reasons why organisations or individuals opt for a
particular form.

Performance outcome 4
Working in small groups, learners will need to be given projects with pre-prepared scenarios of network
requirements that will allow them to identify outline document content as identified in the unit content.
If at all possible, a local organisation (or even the learner’s own organisation) that has a straightforward
network learners could work on, with the outcome being judged by the organisation, would be an ideal
scenario. It is important that the learner adheres to the requirements of the unit content, to ensure that
they develop the skills required to be a network engineer or support technician.
Performance outcome 5

This outcome could be linked directly to the project work in Performance outcome 4. All networks will have issues eventually, but they are very likely to occur while they are being built. That is why testing always takes place during and at the end of a network build. When learners have completed the network in Performance outcome 5, the testing required to ensure the network is working correctly would meet the requirements of this performance outcome. However, should this not be possible, then learners should have access to a training or development network that can be altered to introduce errors, which the learners can then identify, test and correct.

Possibly in small groups, learners could identify a range of benchmarking standards and diagnostic tools for a range of different faults. The wider group could discuss the different choices and decide whether they were appropriate, and which approach would be the most efficient and effective.

Learners could discuss the importance of testing through class discussions or discussions with visiting technical speakers and also identify which would be the most appropriate tests for the installation of hardware and software required to build the computer system in Performance outcome 4. From this, there could be discussion of benchmarking standards and benchmarking software and the importance of benchmarking to identify the quality of the performance of the system. The learner should have the opportunity to discuss the range and role of diagnostic tools in identifying issues with a computer system. This may be the result of issues with the system they are building or machines that have been prepared to allow the learner to find and repair a range of hardware and software faults. If learners had a chance to work with technical staff, this opportunity may arise naturally.

Error codes and messages should also be investigated and learners should discuss how to interpret these, what they mean and where to seek clarification (as some error messages merely refer to error code ‘xxxxxxxxxx’ which gives no clue to the issue).

Learners could also research different testing documentation and their content, and as a group discuss in class why it is important to be able to identify failed as well as successful installations, repairs or upgrades. Learners should also discuss how they would identify when to report any problems to a senior colleague if the tests should fail or whether they can rectify the problem themselves.

Performance outcome 6

Learners will need access to a real network in the work place, as part of a work placement or through a training or development lab network.

Learners should have the opportunity to carry out maintenance activities for the maintenance cycle and complete all necessary upgrades, updates, documentation etc. This practical activity is important and thus a learner must take this responsibility over a period of time to ensure that they have the opportunity to engage with a range of maintenance activities.

Synoptic assessment guidance

Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development, which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.
P1: Describe nine activities which are supported by networks

Unit 1 – AO1: Identify the different types of computer
In this unit learners identify the different types of computers and their common applications for personal and business use. Networking activities will often represent a large overlap with these, eg business application software, e-business and social networking and may lead the learner to describe the nine needed.

Unit 2 – AO4: Understand the fundamentals of computer networks
This unit focuses on communication technologies and as such learners should begin to appreciate the rewards associated with networking; network activities studied here dovetail neatly with this grading criterion, particularly shared resources and improved communication facilities.

P2: Describe four architectures

Unit 1 – AO5: Understand how computers process user requirements
This assessment outcome provides background learning to the data sizes and metrics used by many of the different network architectures and technology types that this grading criterion is seeking. It should also exercise learners’ numeracy skills.

Unit 2 – AO4: Understand the fundamentals of computer networks
This assessment outcome provides additional categorisations of network types, particularly in terms of different network topologies, which are essential aspects of any network architecture and should support the learner completing this criterion.

Unit 5 – PO1: Work with number systems
Number systems fundamentals, base conversion, arithmetic, computer use of bases
Complementing the data sizes and metrics detailed in Unit 1, this unit’s first performance outcome concentrates on working with different number systems, explaining how they work and how they are used in modern computing. Many of these applications include network related concepts that may help the learner respond accurately and confidently when describing the attributes of each of the four architectures. It should also exercise learners' numeracy skills.

P3: Identify the network components for a defined user need

Unit 2 – AO1: Understand the fundamentals of data communication
This grading criterion typically involves consideration of available network components and their bandwidths (as this has a direct impact on network use and performance). This assessment outcome specifically focuses on bandwidth metrics, speeds, limitations and management, all of which should provide rich additional coverage of the core concepts.

Unit 2 – AO2: Analyse data communication methods
This assessment outcome explores the different communication methods that underpin network communications. Transmission media and their features can be explored through this assessment outcome, which is particularly important for helping the learner to select appropriate cables, converters and connectors when identifying network components for a defined need.

P4: Research and map different types of network technologies

P5: Using research describe the main characteristics and properties of two WAN and two LAN technologies

Unit 2 – AO4: Understand the fundamentals of computer networks
Mapping different types of network technologies, particularly in terms of their physical and logical topologies, can be supported by this assessment outcome where various topologies are considered.
P10: Describe five testing techniques
P11: Identify at least three network faults on a selected system

Unit 1 – AO2: Understand and evaluate the hardware requirements of a computer system
This learning outcomes features coverage of the basic input output system (BIOS) in a typical computer system. The learner may find that the use of the BIOS test functionality, eg checking an integrated LAN/Network interface card, proves to be a viable technique.

Unit 1 – AO3: Evaluate the software requirements of a computer system
Testing a network often involves different software-based techniques. This assessment outcome focuses on software utilities used to diagnose and report network problems and could contribute to the learner’s response.

Unit 5 – PO3: Calculate with sequences, series, probability and recursion
Substitution or elimination of faulty components represents two of the core testing techniques that are being tested by this grading criterion. The use of probability (and related calculations) can provide empirical support to judgements made by the learner; these techniques are found in this unit. It should also exercise learners’ numeracy skills.

Unit 5 – PO4: Gather and interpret data in a meaningful manner
Benchmarking is a core testing technique that can be used when networks are being examined for faults and performance. Data gathering, probability, eg from speed tests, benchmark metrics, packet drops and response time may be gathered and interpreted as quantitative data. It should also exercise learners’ numeracy skills. The P11 performance outcome should provide the learner with the statistical techniques for identifying network faults from captured data.

Useful links and resources

Journals
- Computer networks (Elsevier).
- EURASIP journal on wireless communications and networking (Springer).
- International journal of networking and computing (Elsevier).

Books

Standards
12.4 Unit 4: Network threats and vulnerabilities

<table>
<thead>
<tr>
<th>Title</th>
<th>Network threats and vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>A/507/6433</td>
</tr>
<tr>
<td>Unit assessment type</td>
<td>Centre assessed and externally quality assured</td>
</tr>
<tr>
<td>Recommended assessment method</td>
<td>Practical assignment</td>
</tr>
<tr>
<td>This is the preferred assessment method for this unit. A centre may choose an alternative method of assessment, but will be asked to justify this as part of the quality assurance process.</td>
<td></td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>Communication (oral)</td>
</tr>
</tbody>
</table>

- Ideally this unit should be taught using a quarantined network with associated media and network interconnection devices. In addition client and server PCs are required that grant the learners full administrative access; ideally these should encompass multiple operating systems, eg Microsoft Windows and a suitable Linux distribution.

- A range of software hacking tools are required including (for example) ARP cache poisoning tools and password cracking/recovery.

- Installed services are also key, particularly web servers (eg Apache and Microsoft IIS) and network aware relational databases (MySQL, Microsoft SQL server etc). A variety of web browser clients may be beneficial (particularly those with good inspection/debugging facilities), as are bespoke web applications with known/deliberate insecurities (making them ideally vulnerable to exploitation and learner experimentation).

- A range of network security tools such as firewalls, VPNs, IDS, self-signed certification generators etc are also recommended. Many of these software products can be found through open source licensing.

<table>
<thead>
<tr>
<th>Synoptic assessment within this unit</th>
<th>IT: Cyber Security linked to Units 1, 2 and 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT: Cyber Security and Security Administration linked to Units 1, 2, 3, 6, 7 and 8.</td>
<td></td>
</tr>
<tr>
<td>Draws on underlying principles of security-based software application and utilities as discussed in Unit 1.</td>
<td></td>
</tr>
<tr>
<td>Units 2 and 3 provide the learner with the underlying principles of data communication and the technologies used to build networks, as such many of the building blocks of any secured networked solution are introduced here.</td>
<td></td>
</tr>
<tr>
<td>Units 6, 7 and 8 examine network threats from the contrasting-but-connected perspectives of administration, access to data and programming respectively. Each adds contextual depth to the threats, vulnerabilities and security measures being introduced in this unit.</td>
<td></td>
</tr>
<tr>
<td>A signposted breakdown can be found in this unit’s synoptic assessment guidance.</td>
<td></td>
</tr>
</tbody>
</table>

Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.
Aim and purpose
The aim of this unit is to equip learners with the knowledge and skills to counteract internal and external threats to networks.

Unit introduction
Organisations of all types and sizes as well as end users as individuals, face a very significant risk that malicious individuals could breach their critical computing and data assets Therefore, it is important that IT professionals are able to recognise and manage the threats and vulnerabilities that can exist on all types of network.

A threat can be defined as any potential danger to the confidentiality, integrity or availability of information or systems. Most experts classify network security threats in two major categories: logic attacks and resource attacks. Logic attacks are known to exploit existing software bugs and vulnerabilities with the intent of crashing a system. Resource attacks are intended to overwhelm critical system resources such as CPU and RAM.

A vulnerability can be described as a weak point in network security that can be exploited because of an ineffective or absent safeguard. For example, a poorly configured server or network router provides an attacker with viable opportunities.

Only by understanding and recognising security threats and vulnerabilities can the learner understand how to achieve the business imperatives of networking: enhanced productivity, data integrity, availability and cost effectiveness.

This unit provides the learner with the opportunity to understand the key principles of network security and how networks can be exploited both internally and externally. Within the unit learners will be given the opportunity to conduct risk assessments, use network tools and understand the impact that insecure networks have on organisations.
Unit content

Network security testing

- Tools, eg:
  - banner grabbing
  - vulnerability scanner
  - honeypots
  - honeynets
  - passive vs active tools
  - port scanner
  - protocol analyser
  - 802.11a/b/g WEP and WPA cracking suite
  - automated web application attack suite
  - network discovery tool.

- Areas of testing:
  - perimeter:
    - firewall
    - network based antivirus
    - virtual private network (VPN) encryption
  - network:
    - Network Intrusion Detection System (NIDS)/Intrusion Prevention system (IPS)
    - vulnerability management system
    - network access control
    - access control/user authentication
  - host:
    - Host Intrusion Detection System (HIDS)/Intrusion Prevention system (IPS)
    - host vulnerability assessment
    - network access control
    - antivirus
    - access control/user authentication
  - application:
    - application shield
    - access control/user authentication
    - input validation
  - data:
    - encryption
    - access control/user authentication.
Analysing security issues for a network

External threats and vulnerabilities

- Malware (eg):
  - virus
  - spyware
  - adware
  - back doors
  - polymorphic
  - trojan
  - worm
  - ransomware, eg CryptoLocker.

- Types of threats (eg):
  - eavesdropping:
    - open network
    - Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access 2 – Pre-shared Key (WPA2-PSK)
    - captive portal.
  - data modification
  - spam
  - phishing (including spear phishing)
  - pharming
  - Denial-of-Service attack (DoS Attack)
  - Distributed Denial of Service Attack (DDoS Attack):
    - jamming/interference
    - authentication/association flooding
    - de-authentication flooding
    - Extensible Authentication Protocol (EAP) attacks.
  - man-in-the-middle attacks:
    - ARP and DNS Poisoning
    - captive portal (Evil Twin)
    - 802.1X/EAP.
Analysing security issues for a network

External threats and vulnerabilities continued

- cypher attacks:
  - WEP
  - WPA-PSK Dictionary
  - WPA-TKIP
  - session hijacking
  - flash cookies
  - cookies and attachments
  - malicious add-ons
  - compromised key attack
  - password attack
  - network sniffing
  - application layer attack
  - Identity spoofing (IP address spoofing)
  - URL hijacking
  - client-side attacks
  - smurf
  - SYN Flood
  - SQL Injection attack
  - fraggle
  - bluesnarfing
  - rogue access point
  - snorting or Sniffing.

- Risks:
  - risk assessment of the likelihood of attack based on the identified vulnerability.

- Exploits, eg:
  - client side
  - server side
  - scanner
  - module
  - payload
  - trigger
  - injection
  - pivoting
  - spoof
  - shell code.
| Internal threats and vulnerabilities | • Unauthorised access.  
| | • Accidental damage:  
| |   • localised disasters eg fire, water leak  
| |   • human error  
| |   • technical error.  
| | • Equipment failure or damage.  
| | • Theft or loss of data.  
| | • Unauthorised modification of data.  
| | • Shoulder surfing.  
| | • Accidental disclosure or deletion.  
| | • Actions of disgruntled employees:  
| |   • intentional disclosure or deletion  
| |   • malicious damage  
| |   • industrial espionage.  
| | • Carelessness, eg sensitive data on portable devices (USB etc).  
| Other external threats | • Natural disasters eg fire, flooding, lightning, earthquake etc.  
| | • Dumpster diving.  

### Analysing security issues for a network

<table>
<thead>
<tr>
<th>Specific threats to web server and web applications</th>
<th>Specific threats to database server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web server attack vectors, eg:</strong></td>
<td><strong>Unauthorised access.</strong></td>
</tr>
<tr>
<td>- source code reveal (bad server configuration)</td>
<td><strong>Poorly configured user access and set permissions.</strong></td>
</tr>
<tr>
<td>- non-patching of flawed code, eg 'Heartbleed'</td>
<td><strong>Poorly configured web management, eg PHPmyadmin.</strong></td>
</tr>
<tr>
<td>- poor session management, eg no timeout, invalidation</td>
<td><strong>Use of unencrypted sensitive data at rest (eg user authentication credentials).</strong></td>
</tr>
<tr>
<td>- broken authentication, eg sessionID reveal in URL</td>
<td><strong>Lack of regular backup regime.</strong></td>
</tr>
<tr>
<td>- poor security management, eg use of unpatched, out of date and vulnerable frameworks which are exposed</td>
<td></td>
</tr>
</tbody>
</table>
### Deploying secure networks

**Different forms of network defence**

- **Network organisation, eg:**
  - virtual private network (VPN)
  - subnets
  - virtual local area networks (VLANs)
  - private local area networks (PVLANs).
- **Software and hardware solutions, eg:**
  - firewalls (software-based and dedicated hardware)
  - proxy server
  - intrusion detection system (NIDS or HIDS)
  - network based antivirus
  - internet content filter, eg protocols, attachments etc.
  - spam filter (blacklist, whitelist)
  - URL filter (blacklist, whitelist)
  - web content filter, eg keywords etc.
  - malware inspection
  - NAP with dynamic host configuration protocol (DHCP) enforcement
  - secure/multipurpose internet mail extensions
  - remote authentication dial-in user service (RADIUS)
  - diameter.
- **Configuration and hardening, eg:**
  - session timeout periods
  - change default passwords
  - static vs. dynamic IP addresses
  - non-broadcast of SSID
  - use of non-standard ports for network services
  - quality of service (QoS)
  - logging access and activity
  - multifactor authentication.

### Apply security settings to network technologies

**Awareness of VPN and tunnelling protocols**

- Virtual private networks.
- Open-source VPN.
- Tunnelling protocols.

**Firewall configuration**

- Commercial and open source solutions.
- Bespoke hardware firewalls.
- Active threat management.
- Network address translators (NATs).
- White and black lists.
- Blocking by:
  - protocol
  - port
  - IP address (source or destination)
  - MAC address (source or destination).
### Apply security settings to network technologies

| Switch configuration | • Implementing virtual local area networks (VLANs).  
|                      | • Protection from loops, ie using Spanning Tree Protocol (STP).  
| Antivirus configuration | • Frequency of virus signature updates.  
|                       | • ‘On demand’ scanning settings for downloads and email attachments.  
|                      | • Scanning frequency.  
|                      | • Integration with operating systems and email systems.  
| Domain configuration | • Authentication of users.  
|                      | • Authorisation of users.  
|                      | • User permissions and default behaviours.  
|                      | • Creation, maintenance and application of group security policies.  
|                      | • Bandwidth throttling.  
|                      | • Roaming user profiles and desktops.  
|                      | • Remote Desktop Services (RDS).  
|                      | • Remote Desktop Protocol (RDP).  
| Web technology security and configuration | • Awareness of WAMP, LAMP, MAMP stacks.  
|                      | • Web server configuration:  
|                      | • suppressing web server footprint (eg name, version etc)  
|                      | • aliases and virtual hosts  
|                      | • ports for HTTP/HTTPS traffic (eg 80, 443, 8080 etc)  
|                      | • automatic HTTP to HTTPS directs  
|                      | • session timeout constraints  
|                      | • allowed/blocked IP ranges  
|                      | • suppressing directory views  
|                      | • directory/folder permissions  
|                      | • file permissions  
|                      | • file type execution (eg ASP .Net, .ASP, .PHP etc)  
|                      | • suppressing web application code errors  
|                      | • limit maximum concurrent connections.  
|                      | • File Transfer Protocol (FTP) (client) access:  
|                      | • allowed/blocked IP ranges  
|                      | • use of FTPS (also known as FTP-ES, FTP-SSL and FTP Secure).  
|                      | • Secure Shell (SSH) remote access.  
|                      | • Relational database remote access and authorisation:  
|                      | • allowed/blocked IP ranges  
|                      | • non-standard ports  
|                      | • user permissions, especially for DDL and DML SQL statements  
|                      | • limit maximum concurrent connections  
|                      | • securing web-based front-ends, eg PHPmyadmin.  
|                      | • Web application configuration and deployment.  
|                      | • Web browser client security (eg security settings, plug-ins etc).  

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
### Apply security settings to network technologies

| Digital certification | • Types of certificate, ie self-signed, CA-issued, different vendor classes.  
| | • Contents of a digital certificate.  
| | • Public key infrastructure (PKI).  
| | • Certificate authority (CA).  
| | • Creating self-signed certificates.  
| | • Deploying keys and certificates.  
| | • Operating system management, eg windows active directory certificate services, Mac OS X Keychain etc.  
| Software maintenance | • Using cryptographic hashes to confirm file integrity, eg MD5, SHA etc.  
| | • Patching applications.  
| | • Updating code libraries.  
| | • Network deployment of software.  

### Business continuity planning to mitigate risks and impact on organisations caused by insecure networks

| Ethical responsibilities of a cyber security professional | • Professional responsibility to assure the reliability, accuracy, availability, safety and security of all aspects of information and information systems in their care.  
| | • Important of continuing professional development (CPD).  
| | • Awareness of alerts and advisories, eg Microsoft, OWASP, CISP, open source, CVE etc.  
| | • Balance of individual privacy and security needs.  
| | • Membership of professional bodies, eg information systems security association (ISSA).  
| Organisational impact | • Losses (eg):  
| | • service or impacted service  
| | • intellectual property  
| | • sensitive data or information  
| | • current business or income  
| | • potential business or contracts  
| | • property  
| | • professional reputation  
| | • customers  
| | • suppliers.  
| | • Increased costs.  
| | • Bad publicity.  

Visit [aqa.org.uk](http://aqa.org.uk) for the most up-to-date specification, resources, support and administration.
### Business continuity planning to mitigate risks and impact on organisations caused by insecure networks

<table>
<thead>
<tr>
<th>Business management</th>
<th>Planning to manage risks and vulnerabilities</th>
</tr>
</thead>
</table>
| • Analysing risk severity:  
  • low  
  • medium  
  • high.  
| • Regulations.  
| • Probability:  
  • unlikely  
  • likely  
  • very likely.  
| • Procedure.  
| • Objectives:  
  • prevent interruption of mission-critical services  
  • minimise disruption  
  • re-establish full business functions quickly and smoothly.  
| • allocating budget accordingly  
| • utilising new technologies and failover mechanisms.  
| • Business continuance plan containing:  
  • disaster recovery plan  
  • business resumption plan  
  • business recovery plan  
  • contingency plan.  
| • Key concepts:  
  • identifying critical (and essential) business functions  
| • Business continuance plan containing:  
  • disaster recovery plan  
| • allocating budget accordingly  
| • utilising new technologies and failover mechanisms.  
| • Business continuance plan containing:  
  • disaster recovery plan  
  • business resumption plan  
  • business recovery plan  
  • contingency plan.  
| • Objectives:  
  • prevent interruption of mission-critical services  
  • minimise disruption  
  • re-establish full business functions quickly and smoothly.  
| • Business continuance plan containing:  
  • disaster recovery plan  
  • business resumption plan  
  • business recovery plan  
  • contingency plan.  
| • Probability:  
  • unlikely  
  • likely  
  • very likely.  
| • Business continuance plan containing:  
  • disaster recovery plan  
| • Objectives:  
  • prevent interruption of mission-critical services  
  • minimise disruption  
  • re-establish full business functions quickly and smoothly.  
| • Business continuance plan containing:  
  • disaster recovery plan  
  • business resumption plan  
  • business recovery plan  
  • contingency plan.  
| • Probability:  
  • unlikely  
  • likely  
  • very likely.  

- **Business management**
  - Analysing risk severity:
    - low
    - medium
    - high.
  - Probability:
    - unlikely
    - likely
    - very likely.
  - Loss:
    - minor
    - moderate.
  - Objectives:
    - prevent interruption of mission-critical services
    - minimise disruption
    - re-establish full business functions quickly and smoothly.
  - Key concepts:
    - identifying critical (and essential) business functions
    - allocating budget accordingly
    - utilising new technologies and failover mechanisms.
  - Business continuance plan containing:
    - disaster recovery plan
    - business resumption plan
    - business recovery plan
    - contingency plan.

- **Planning to manage risks and vulnerabilities**
  - Regulations.
  - Procedure.
  - Baseline.
  - Guideline.
  - Layering.
  - Education.
  - Backup and recovery strategies.
  - Upgrading.
  - Setting up file and folder permission.
  - Principle of least privilege.
**Performance outcomes**

On successful completion of this unit, learners will be able to:

<table>
<thead>
<tr>
<th>Performance outcome 1:</th>
<th>Understand network security testing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance outcome 2:</td>
<td>Analyse security issues for a network.</td>
</tr>
<tr>
<td>Performance outcome 3:</td>
<td>Deploy secure networks.</td>
</tr>
<tr>
<td>Performance outcome 4:</td>
<td>Apply security settings to network technologies.</td>
</tr>
<tr>
<td>Performance outcome 5:</td>
<td>Plan for business continuity to mitigate risks and impact on organisations caused by insecure networks.</td>
</tr>
</tbody>
</table>

**Grading criteria**

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO1: Understand network security testing</strong></td>
<td>To achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td>P1</td>
<td>Identify five network security testing tools.</td>
<td>M1</td>
<td>Explain and demonstrate how you might use three different network security testing tools.</td>
</tr>
<tr>
<td>P2</td>
<td>Describe the five key areas of testing on a network.</td>
<td>M2</td>
<td>Explain three different types of Access Control/User Authentication methods that can be used to gain access to network.</td>
</tr>
<tr>
<td><strong>PO2: Analyse security issues for a network</strong></td>
<td>P3</td>
<td>Create an inventory of five vulnerabilities associated with wireless networks with brief descriptions of each.</td>
<td>D1</td>
</tr>
<tr>
<td>P4</td>
<td>Carry out a technical reconnaissance using appropriate network discovery tools to scan an identified network and collect configuration and security data.</td>
<td>D2</td>
<td>Evaluate the effectiveness of three different types of Access Control/User Authentication methods that can be used to gain access to network.</td>
</tr>
<tr>
<td>Performance outcomes</td>
<td>Pass</td>
<td>Merit</td>
<td>Distinction</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>To achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td>PO3: Deploy secure networks</td>
<td>P5 Demonstrate <strong>five</strong> internal threats and <strong>five</strong> external threats to an organisation’s network security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO4: Apply security settings to network technologies</td>
<td>P6 Demonstrate <strong>two</strong> specific threats to web servers, web applications and database servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P7 Identify the hardware and software components required to establish a secure network.</td>
<td>M3 Discuss three configuration or hardening options that could be employed when deploying a secure network.</td>
<td>D3 Evaluate a secured network.</td>
</tr>
<tr>
<td></td>
<td>P8 Describe <strong>five</strong> different types of configuration that can affect network security.</td>
<td>M4 Demonstrate changes to the configuration of three different devices, services or technologies that improve network security.</td>
<td>D4 Evaluate the effectiveness of the configuration changes made to improving network security.</td>
</tr>
<tr>
<td></td>
<td>P9 Create a digital self-certificate for a given purpose and test it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P10 Perform <strong>two</strong> different software maintenance tasks that demonstrate improved security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO5: Plan for business continuity to mitigate risks and impact on organisations caused by insecure networks</td>
<td>P11 Describe the ethical responsibilities of a cyber security professional.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Visit [aqa.org.uk](http://aqa.org.uk) for the most up-to-date specification, resources, support and administration.
### Performance outcomes

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td>P12</td>
<td>Describe the possible organisational impact caused by a compromised network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P13</td>
<td>Carry out a risk assessment on a selected network system.</td>
<td>M5 Explain how decisions on risk severity were made for the selected network system.</td>
<td>D5 Evaluate the effectiveness of the risk assessment process when applied to a selected network system.</td>
</tr>
<tr>
<td>P14</td>
<td>Create a business continuance plan for a selected network system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P15</td>
<td>Present your business continuance plan.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Assessment amplification

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

In completing performance criteria P15, learners will be presented with an opportunity to demonstrate the transferable skill of communication (oral).

Learners could use scenarios that cover a range of performance outcomes. If learners have the opportunity to have a work placement or a job in network support then they may be able to use the evidence from these activities for some or all of the performance criteria.

Learners could be provided with access to an actual network system and /or detailed case studies or scenario to analyse. If an actual network system is available it should provide learners with opportunities to identify any potential risks and vulnerability.

For P1 the learners should identify five network security testing tools across the range, explaining and demonstrating how they might use three for M1. D1 the learner is required to ‘evaluate the effectiveness of three different network security tools’. Before attempting this criterion discussions need to take place between the learner and tutor as to how a hacker views a system and anticipate how things could be exploited to gain unauthorised access.

P2 requires learners to describe key areas of the network that can be tested.
M2 requires the learner to explain three different types of access control/user authentication methods that can be used to gain access to network.

For D2 the learner is asked to ‘evaluate the effectiveness of three different types of access control/user authentication methods that can be used to gain access to network’. The learner and tutor therefore need to discuss how secure is the first user interface element most subjects encounter when accessing an information system.

For P3 this criterion requires the learner to create an inventory of five vulnerabilities associated with wireless networks with brief descriptions of each.

For P4 the learner should carry out a technical reconnaissance using the appropriate tools to scan an identified network and collect configuration and security data. Again evidence for the criterion can be presented in the form of a presentation with a video and commentary) combined with an illustrated short report which would include appropriate tables.

For P5 the learner should research, outline and demonstrate how five external and five internal threats to network security can be managed. Evidence for this criterion can be presented as either presentation or via documented practical’s.

For P6 the learner is required to demonstrate two specific threats to security. The threats must be network related and involve either a web server, a web application or a database server.

For P7 the learner is required to identify the hardware and software components that are required to establish a secure network. Discussion and research should form the bases for this criterion.

M3 criterion will require the learner to discuss three software configurations or hardware options that could be employed when deploying a secure network. For instance measures such as configuring a virus scan, installing and configuring a firewall, setup security options in internet options, etc.

P8 requires the learner to ‘describe five different types of configuration that can affect network security. This criterion is asking the learner to explore different types of hardware (routers, switches) and different types of software (firewalls, virus scanners) in order to understand the different ways of configuring both software and hardware in order to make a network secure. Both M4 and D4 are extensions of this pass and require the learner to expand on the knowledge gained in the pass.

P9 requires the learner to create a digital certificate. There are many ways in which a digital certificate can be created and the tutor will need to provide a given purpose for the certificate. After discussion with the tutor learners will produce a digital certificate, document it and test it.

P10 requires the learner to ‘Perform two different software maintenance tasks that demonstrate improved security’ this criterion can be seen as an extension to P8. Port Scanning, PING ect can be used here.

P11 requires the learner to research, discuss and describe the responsibilities of a cyber security professional.

For P12 learners should identify and describe the organisational impact of an insecure network as described in the unit content.

P13 requires the learner to carry out a risk assessment on a selected network. A real or virtual network can be the selected network.

M5 requires the learner to explain how decisions on risk severity were made for the selected network system. A discussion about ‘risk matrices’ probability and impact scales will help the learner to explain and evidence this criterion.
D5 is an extension of M5 and asks the learner to evaluate the effectiveness of the risk assessment process when applied to a selected network system (virtual or real). This criterion requires the learner to evaluate the process of risk analysis/assessment as it has been applied to a network. Learners should be encouraged to look at both Quantitative and Qualitative risk assessments. Discussion of the ‘Quantitative Risk Analysis Formula’ may also help to prepare the learner to achieve this criterion.

P14 and P15 are combined objectives that require the learner to discuss, research and create a business continuity plan (based on a real or virtual network) and then the learner has to present the plan to his tutor and peers. Evidence for P15 can be the presentation, video and observation. The formal documentation to support this skill should be used, and the presentation should be of the required length.

Employer engagement guidance
The institution could engage with local employers and their own network staff to provide staff to discussion networks with learners and provide work based opportunities or cases, scenarios and projects that learners could use for training and assessment purposes.

The British Computer Society (BCS) and the European arm of the Association for Computing Machinery, for example, may be willing to engage with learners in discussions on networking.

Delivery guidance

General comment
Learners studying this module would benefit from having studied Unit 2 Communication technologies.

The assessment criteria could be delivered holistically rather than as discrete elements through project work or work placement opportunities.

It would be very useful if learners could engage in work placement activities for this unit, if this is not possible then the learner must have access to a network development or training facility in order to carry out the design, build and testing activities which are essential elements of this unit.

Performance outcome 1
Learners could carry out research in small groups, class discussions or visits to, or discussions with, network specialists within the organisation or with external institutions.

Performance outcome 2
Learners could investigate a range of networks such as those within the institution, a local organisation, or their own home networks and feed this back to the group in order to consolidate an agreed understanding of the topologies. From these discussions the learners could, as a group, identify network security issues.

Performance outcome 3
Either individually or in small groups, learners could set up or examine a secure network and identify the hardware and software components required to establish a secure network.

Performance outcome 4
Learners to gain this outcome will be required to perform two different software maintenance tasks that demonstrate improved security. They will create a digital self-certificate and test it.
Performance outcome 5
Learners working in small groups are required to research and report on the ethical responsibilities of a cyber security professional. The learners take the threats identified in PO2 and discuss the impact and risk to an organisations network. Evidence will be individually produced and take the form of a short report and presentation for management.

Synoptic assessment guidance
Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development, which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

P1: Identify five network security testing tools
Unit 1 – AO3: Evaluate the software requirements of a computer system
Testing a network requires a number of different techniques; many of these are software-based. This assessment outcome focuses on different types of software, especially utilities that are often used to diagnose network problems.

P2: Describe the five key areas of testing on a network
Unit 3 – PO2: Identify the different types of network architectures and technology types
Many of the areas of testing (perimeter, network, host, application and data) are introduced in this unit. Definitions and coverage in this unit should contribute to the learner being able to not only identify the five areas required but also identify the different types of technology they employ.

P4: Carry out a technical reconnaissance using appropriate network discovery tools to scan an identified network and collect configuration and security data
Unit 2 – AO1: Understand the fundamentals of data communication
Unit 2 – AO2: Analyse data communication methods
Unit 2 – AO3: Analyse basic mobile technology communication
Unit 2 – AO4: Understand the fundamentals of computer networks
Unit 2 – AO5: Understand network conceptual models, protocols and devices
Auditing the network and system components required as part of a technical reconnaissance involves using subject specialist terminology correctly. The majority of these communication terms and concepts are introduced in this unit.

Unit 3 – PO2: Identifying the different types of network architectures and technology
Many of the network and system components present in a technical reconnaissance are introduced in this unit. Definitions and coverage in this unit should contribute to the learner being able to accurately identify the technologies being used within an organisation.
P5: Demonstrate five internal threats and five external threats to an organisation’s network security

Unit 6 – AO1: Explain the fundamentals of cyber attacks
This unit details a number of threats that contribute to common cyber attacks and should offer learners another perspective when identifying and planning to demonstrate internal and external threats to satisfy this criterion.

P6: Demonstrate two specific threats to web servers, web applications and database servers

Unit 8 – PO4: Recognise vulnerabilities and counter threats to website and mobile technologies
This performance outcome, although approaching threats (and vulnerabilities) from a programming perspective, adds extra depth and amplified technical detail that the learner may find advantageous when tackling this performance criterion.

P7: Identify the hardware and software components required to establish a secure network

Unit 1 – AO3: Understand the software requirements of a computer system
In this unit learners are introduced to different types of security software such as firewalls, antivirus, anti-spyware and the concept of encryption and biometrics, providing a solid foundation for this coverage.

Unit 3 – PO2: Identify the different types of network architectures and technology types
Part of this performance outcome focuses on basic network security; the concept of a honeypot is typically introduced here.

Unit 7 – PO1: Select hardware and software to promote security for a network system
This unit’s coverage of intrusion detection and prevention systems may provide supporting evidence to assist the learner’s selection of suitable hardware and software for this grading criterion.

P8: Describe five different types of configuration that can affect network security

Unit 8 – PO4: Recognise vulnerabilities and counter threats to website and mobile technologies
This unit’s performance outcome provides learners with various forms of client side and server side protection that could be used to improve or (if badly performed) degrade network security.

P9: Create a digital self-certificate for a given purpose and test it
P10: Perform two different software maintenance tasks that demonstrate improved security

Unit 8 – PO5: Demonstrate the key features and functions of operating system shell scripting
Some software maintenance tasks may be executed in script form or from the command line interface rather than by executing specialist tools. This performance outcome provides learners with practical experience of doing these tasks and this should ease their completion of this grading criterion.

P11: Describe the ethical responsibilities of a cyber security professional

Unit 8 – PO3: Understand legal issues and standards affecting security
This unit’s examination of legal issues also touches upon the more complex ethical factors which determine the balance between privacy and accessibility of data, something often seen as a key concern for cyber security professionals when informing their approach.
P12: Describe the possible organisational impact caused by a compromised network

Unit 6 – AO1: Understand the fundamentals of cyber attacks

This assessment outcome examines the objectives of cyber attacks. These often signpost the actual impacts felt by the organisation. Learners will undoubtedly benefit from examining and researching publicly documented cyber attacks and their effects.

Unit 6 – AO2: Explain the controls that an organisation needs to implement to manage risks

Organisational impact is a key aspect of the risk management undertaken when analysing the possibility of a compromised network from a cyber attack. Learners may be able to link the need for suitable controls and the possible organisational impacts to substantiate their response for this grading criterion.

Useful links and resources

Books


Websites

- Cisco: [cisco.com](http://cisco.com)
- PuTTY: [chiark.greenend.org.uk/~sgtatham/putty/download.html](http://chiark.greenend.org.uk/~sgtatham/putty/download.html)
- Search Mobile Computing: [searchmobilecomputing.techtarget.com](http://searchmobilecomputing.techtarget.com)
- The OSI Model's Seven Layers: [support.microsoft.com/kb/103884](http://support.microsoft.com/kb/103884)
- Wireshark Protocol Analyser: [wireshark.org/download.html](http://wireshark.org/download.html)
### 12.5 Unit 5: Maths for computing

<table>
<thead>
<tr>
<th>Title</th>
<th>Maths for computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>R/507/6437</td>
</tr>
<tr>
<td>Unit assessment type</td>
<td>Centre assessed and externally quality assured</td>
</tr>
<tr>
<td>Recommended assessment method</td>
<td>Practical assignment</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>N/A</td>
</tr>
<tr>
<td>Resources required for this unit</td>
<td>Suitable Windows PC, Linux, Apple Macintosh OS X, Apple iOS or other suitable platforms that offer access to the low levels of the operating system, eg debug or monitor facilities where RAM address content may be examined; this is often achievable through a virtualised platform. In addition, pathway relevant software should be available that demonstrates the use of different number systems, eg networking software for subnet masks, graphics software for red, green, blue (RGB) colour codes, email clients for MIME Base64 attachments etc. Optional resources are indicated in each assessment outcome that may enhance the learners’ experience in this unit. Learners should also have access to suitable offline and online learning material, manuals, help sheets and coded examples in order to encourage self-sufficiency.</td>
</tr>
<tr>
<td>Synoptic assessment within this unit</td>
<td>IT: Cyber Security and Security Administration linked to Units 1, 2 and 6. Draws on the hardware components of a computer system (specifically the CPU), underlying principles of data concepts and how user requirements are processed, as discussed throughout Unit 1. Some key aspects such as detecting errors in data transmissions can be made using simple binary-based parity checks, as described in Unit 2. A signposted breakdown can be found in this unit’s synoptic assessment guidance.</td>
</tr>
</tbody>
</table>

### Aim and purpose

This unit will provide the learner with the necessary knowledge to understand the mathematical concepts that enable computers to store, process, communicate and transmit data. The learner will also develop a range of skills required to recognise its practical application in everyday computing, process numerical data correctly and interpret data they have collected in a statistical meaningful manner.
Unit introduction
Maths is at the very heart of any computer system; from storing its data to displaying complex imagery on screen or simply loading a web page – maths is the ‘magic’ that makes it happen.

In this unit learners will gain an understanding of how computer internally represent data and make decisions, along with applying common mathematical techniques for creating algorithms that solve set problems, whether these are presented in terms of system, networking or programming situations.

The unit begins with a sound foundation in the number systems that are prevalent in the operation of computer hardware, software and systems. It then examines the underlying logic used in the digital circuits that power the micro-processors inside the computer; logic that is used every day by operating systems, networks and programmers alike.

Once the fundamental building blocks have been locked into place, it is possible to investigate the practical use of maths in computing, focussing on popular applications such as number series, recursion, probability and matrix manipulation.

Unit content

Working with number systems

| Number systems fundamentals | • Concept of a positional numeral system, eg positional weights.  
|                           | • Base or radix terms; correct mathematic notational use, eg 122. 
|                           | • Base notation in computing, eg # or 0x prefix for hexadecimal.  
|                           | • Common computer bases:  
|                           |   • denary (Base 10)  
|                           |   • binary (Base 2)  
|                           |   • octal (Base 8)  
|                           |   • hexadecimal (Base 16)  
|                           |   • larger, eg multipurpose internet mail extensions (MIME) Base 64.  
| Base conversion | • Base conversion methods:  
|                |   • denary to binary and vice versa  
|                |   • binary to hexadecimal and vice versa  
|                |   • denary to hexadecimal and vice versa.  
| Fractional and negative integers in binary | • Binary integer signing techniques:  
|                                            |   • unsigned  
|                                            |   • sign and magnitude  
|                                            |   • one’s complement  
|                                            |   • two’s complement.  
|                                            | • Representing fractional values in:  
|                                            |   • denary  
|                                            |   • binary.  
|                                            | • Fixed number storage in binary.  
|                                            | • Floating point number storage notation in Binary, ie significant/mantissa, exponent etc.  
|                                            | • Single and double precision.  

### Working with number systems

#### Base arithmetic
- Performing basic arithmetic operations in other bases; binary, hex etc:
  - addition
  - subtraction
  - multiplication
  - division.

#### Computer use of bases
- Common use of different bases in modern computing, eg:
  - binary, eg:
    - internal data representation
    - Boolean logic and flags
    - internet protocol subnet masks
    - Classless Inter Domain Routing (CIDR) notation
    - character representation, eg 7 or 8 bit American Standard Code for Information Interchange (ASCII) characters etc
  - octal, eg
    - Unix/Linux CHMOD file permissions
    - escape strings, UTF-8
  - hexadecimal, eg
    - error codes
    - network (Media Access Control) MAC physical addresses
    - memory (eg RAM) addresses
    - 8-bit per channel RGB (Red Green Blue) colour codes, eg #FF0000 = red
    - internet uniform resource identifier (URI).
- Binary vs Gray code, rationale and use.

### Understanding and applying computer logic

#### Foundation of computer logic
- Boole, Boolean logic/algebra (true, false; 1,0).

#### Basic logical operators
- Processing and outputs of basic logical operations:
  - And (conjunction)
  - Or (disjunction)
  - Not (negation).
- Common logical operator symbols.

#### Composition and derived operators
- Processing and outputs of derived logical operations:
  - Exclusive or (EOR or XOR)
  - Negative or (NOR)
  - Negative and (NAND)
  - Exclusive Negative or (XNOR).
- Common logical operator symbols.
### Understanding and applying computer logic

#### Visual representation of logical operations
- Representing logic in diagrammatic form:
  - truth tables for each using x and y as inputs
  - digital logic gate diagrams for circuits
  - Venn diagrams.
- Creating circuits using only one type of logic gate, eg NOR or NAND.

#### Working with Boolean algebra
- Notation and symbols
- Interpreting simple equations, eg $(x,y) + x$
- Interpreting complex equations, eg $(x+y, x) + (x,y)$
- Common techniques used to simplify complex Boolean expressions:
  - Boolean identities
  - De Morgan’s Laws
  - Karnaugh maps
  - truth tables.

### Calculating with sequences, series, probability and recursion

#### Sequence and series
- Sequences:
  - type, eg finite or infinite
  - notation, $n^{th}$ term
  - rules and finding rules
  - term and term number
  - arithmetic and geometric sequence.
- Series:
  - definition, contrast to a sequence
  - use of sigma ($\sigma$) notation.

#### Probability
- Probability terminology and usage, eg:
  - probability definition
  - probability line
  - experiment or trial
  - sample space and sample point
  - events and event types (dependent, independent, mutually exclusive).
- Space diagrams eg ‘double’ values when two dice are thrown.
- Visualising events, eg using Venn diagrams (mutually exclusive events), tree diagrams (dependent events).
### Calculating with sequences, series, probability and recursion

**Recursion**
- Series eg Fibonacci, factorial.
- Rules of recursion:
  - have a base case
  - state change toward base case
  - must call itself.
- Common recursive algorithms used in computing, eg
  - factorial, quicksort, binary search, directory traversal, Sierpinski triangle.
- Instances where simple iterative techniques may be more efficient.

### Gathering and interpreting data in a meaningful manner

**Gathering data**
- Primary and secondary data.
- Quantitative and qualitative data.
- Common methods of gathering data, eg real world measurements, observation, questionnaires, surveys etc.
- Extraction of required information from raw data.
- Limitations of data gathered, eg accuracy, sample size, need for cleaning invalid data points (eg extreme outliers).

**Representing data**
- Concepts and techniques for comparing data sets:
  - range and range limits
  - averages, eg arithmetic mean, median (middle value), mode (most frequent)
  - relationship between mean, median, mode, eg symmetrical distribution, positive or negative skew
  - cumulative frequency diagrams, statistical dispersion measures, eg interquartile (IQR) range
  - Standard deviation (SD)
  - variance
  - histograms.

**Interpreting data**
- Analysing summary data.
- Identification of trends and recurring patterns.
- Proving a hypothesis.
Applying matrix methods to solve problems

| Matrices | • Matrices to represent ordered data.  
• Matrix terminology, eg rows, columns, elements or entries, subscripts, ‘m-by-n’ size definitions.  
• Forms of matrix:  
  • row vector  
  • column vector  
  • square matrix. |
|---|---|
| Matrix operations | • Basic operations include:  
  • addition  
  • scalar multiplication  
  • transposition. |
| Common matrix applications and techniques | • Common practical applications of matrices, eg:  
  • solving simultaneous equations  
  • transforming vectors; shear, flip, scale and rotate. |

Performance outcomes
On successful completion of this unit, learners will be able to:

| Performance outcome 1: | Work with number systems. |
| Performance outcome 2: | Understand and apply Boolean logic. |
| Performance outcome 3: | Calculate with sequences, series, probability and recursion. |
| Performance outcome 4: | Gather and interpret data in a meaningful manner. |
| Performance outcome 5: | Apply matrix methods to solve problems. |
### Grading criteria

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO1: Work with number systems</strong></td>
<td><strong>P1</strong> Demonstrate an understanding of a positional numeral system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P2</strong> Represent denary unsigned numeric integers in three different bases using correct notation.</td>
<td><strong>M1</strong> Convert a sequence of five unsigned integers between different bases using correct notation.</td>
<td><strong>D1</strong> Convert three different non-denary values required for or generated by a computer for a specific processing purpose.</td>
</tr>
<tr>
<td></td>
<td><strong>P3</strong> Represent signed denary values in binary using two different techniques.</td>
<td><strong>M2</strong> Explain the difference between storing a denary fractional value using fixed and floating point notation.</td>
<td><strong>D2</strong> Analyse the impact on magnitude and accuracy of a stored number using single and double precision numbers.</td>
</tr>
<tr>
<td></td>
<td><strong>P4</strong> Carry out calculations involving the four common arithmetic operations using two different bases.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO2: Understand and apply Boolean logic</strong></td>
<td><strong>P5</strong> Create suitable diagrams to represent the three basic logical operations using correct notation.</td>
<td><strong>M3</strong> Create suitable diagrams to represent four derived logical operations using correct notation.</td>
<td><strong>D3</strong> Design two circuits which solve set logical tasks using only one type of logic gate.</td>
</tr>
<tr>
<td></td>
<td><strong>P6</strong> Interpret a simple Boolean algebraic expression.</td>
<td><strong>M4</strong> Interpret a complex Boolean algebraic expression.</td>
<td></td>
</tr>
<tr>
<td>Performance outcomes</td>
<td>Pass</td>
<td>Merit</td>
<td>Distinction</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>TO achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
<td></td>
</tr>
<tr>
<td><strong>PO3: Calculate with sequences, series, probability and recursion</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P8 Identify and explain an arithmetic and geometric number sequence.</td>
<td>M5 Explain the difference between a series and a sequence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P9 Describe different probability event types using industry examples.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P10 Use suitable diagrams to represent two different probability events.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P11 Identify and describe a simple recursive function.</td>
<td>M6 Demonstrate how recursion is used to process a selected computing task.</td>
<td>D4 Evaluate a recursion function to determine whether a simple iteration may be more efficient.</td>
<td></td>
</tr>
<tr>
<td><strong>PO4: Gather and interpret data in a meaningful manner</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P12 Gather appropriate data for an investigation of a computer related event.</td>
<td>M7 Analyse the data to identify any issues or limitations which need to be considered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P13 Use appropriate techniques to compare two data sets from an investigation of a computer related event.</td>
<td>M8 Analyse the summary data generated.</td>
<td>D5 Prove a hypothesis from the identification of trends and recurring patterns in the summary data generated.</td>
<td></td>
</tr>
</tbody>
</table>
Performance outcomes

<table>
<thead>
<tr>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td>To achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
</tbody>
</table>

P05: Apply matrix methods to solve problems

<table>
<thead>
<tr>
<th>P14</th>
<th>M9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demonstrate the correct use of matrices and matrix notation using industry data.</td>
<td>Perform at least two basic operations successfully on a given matrix.</td>
</tr>
</tbody>
</table>

P15

Apply appropriate matrix techniques to solve an industry problem.

Assessment amplification

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

There is no mandatory division of grading criteria although, as can be seen from the Grading criteria grid, some are naturally linked either by learning outcome or by a developmental theme. Connections between the various pass, merit and distinction criteria can therefore suggest logical assessment grouping but do not necessarily have to be followed.

Finding a single real world scenario that can cover all criteria is difficult, but not impossible. The key to assessment in this unit, as in others, is to make assessment a natural outcome of the learning experience, with skills being assessed at a level appropriate to the learner's level of experience.

Assessments that connect this unit to others via connected tasks are also encouraged and it is possible that evidence produced during work for this unit may be used to provide evidence for criteria in other units.

As with all units, in order to gain a pass grade, learners must generate evidence that meets all listed pass criteria.

For D1 it is necessary for the learner to generate or interpret three non-denary (ie binary, octal or hex) numbers that are critically required for a particular processing aspect of a computer system. Learners should also be able to demonstrate an understanding of how these values are being used in each aspect.

For P9 and P10 it is expected that probability events being investigated will naturally be contextualised for the learner’s study pathway.

For M6 learners must specifically be able to explain, via demonstration, the workings of a recursive algorithm in terms of a well-known computer process. A list of possible processes is provided in Performance outcome 3, but once again, it should not be considered to be exhaustive and practitioners may choose other suitable examples if they prefer.
Demonstrations could be evidenced through such means as presentation, video or role play.

For **P12**, **M7**, **P13**, **M8** and **D5** evidence can be generated by the learner investigating a computer related event; eg for programmes this could be the number of bugs in program code fixed over weekly periods before launch; for networking this could be the number of login errors reported from client PCs. The ultimate goal will be to prove (or possibly disprove) an initial hypothesis by collecting data about the event, summarising it and interpreting the results using appropriate statistical methods. The actual nature of the event may be selected by the learner but the assessor should ensure it is of suitable size and complexity to reflect study at Level 3.

For **P14** and **P15** this would also involve the selection of a real world event that can be represented and solved using matrices. Again care should be taken to ensure that the event or data set chosen is of a size and complexity commensurate with the level of study.

**Employer engagement guidance**

If learners are in the workplace then the centre could ask the employer whether there were any suitable projects that the learners could work on as part of the team. It would be helpful for the employer to be made aware of the sort of skills that the learners have to practice.

**Delivery guidance**

This unit may be delivered by either a maths practitioner with some computing experience or a computer practitioner confident with the maths content presented herein.

It should be taught, where possible, in conjunction with other units such as those covering programming, cyber security, networking or system support themes, depending on the learners’ pathway. For example, Performance outcome 1 integrates well with delivery in Unit 1: Fundamental principles of computing.

Although the individual components have been identified, the order in which they delivered does not have to follow the sequence provided and, although underpinning concepts are introduced in Performance outcomes 1, 2 and 3 a case can be made for delivering Performance outcomes 4 and 5 in either order, especially if they can be planned to coincide with thematically relevant learner activities in other units.

A single case study, if sufficiently complex and contextualised for the learners’ pathway, could be used to deliver this unit; this should allow learners to discover and appreciate how important mathematical skills are when solving real world problems. However, a number of small projects, each targeting a separate performance outcome, could also be used to good effect.

Presentations or discussions by those working in the computing/IT sector pertaining to the learners’ pathway would be advantageous, especially if the importance and relevance of their underpinning mathematical skills could be highlighted.

**Performance outcome 1**

Learners should consider different number systems and their vital use in computing, particularly when contextualised to their learning pathway, eg hexadecimal notation for error codes that system support technicians will be all too familiar with, or the use of binary to work out subnet masks in networking. Each learning pathway has many suitable examples; a sample is provided for illustration.

Learners could locate examples of different number systems being used in computing and be challenged to interpret these in terms of both the converted denary number and its application. A simple example of this might be to examine a computer's memory address, read the hexadecimal or binary value present, convert it to a denary code and then discover the ASCII character that is being stored.
To summarise, learners must be able to interpret, convert and perform basic arithmetic on these values, demonstrating accuracy, correct notation and a working knowledge of how these values may be used or encountered by them in their computing career.

**Performance outcome 2**

Boolean logic can be taught traditionally but comes alive when contextualised through the use of simple logic circuits, whether these are realised in physical kit form or via circuit design software tools.

There is opportunity here for active learning connections to be made with the delivery of computer programming (specifically ‘if’ statements and conditions involving logical operators), in networking (for example, firewall rules) and system support (processor architecture, ALU etc).

Learning opportunities can be driven through creating simple circuits for simple real world applications, eg traffic light systems, lift doors, vending machines etc.

**Performance outcome 3**

Although this outcome aligns most closely with the developmental needs of someone involved in aspects of programming, understanding these topics can be contextualised with little difficulty for each pathway. For example, technicians may discover the probability of particular brands of hard disks failing by examining fault logs; network specialists may learn how DNS queries may be handled in a recursive manner; cyber security specialists may examine virus infection rates etc.

Recursion is best demonstrated through solving simple computer programming tasks, examples of which are listed in the content. For more able learners, differentiated examples could include concepts such as finding square roots using Newton’s method.

**Performance outcome 4**

This performance outcome can be delivered in a completely contextualised manner. Although learners should be able to visualise statistical information through hand-drawn diagrams, electronic means (eg graphs generated by a spreadsheet application) may also be considered.

Ideally a range of data collection techniques should be experienced and evaluated by the user and, ultimately, any data generated must be analysed and suitable hypotheses developed and presented. These are ideal for group-based activities, class presentations and peer review.

**Performance outcome 5**

It is recommended that the standard matrix theory is delivered in a generic manner through practice of the basic operations listed in the content. It is likely that simultaneous equations may be creatively engineered for each discipline to solve problems with two unknowns, eg for networking it may be ‘time’ and ‘packets lost’, for user support it may be ‘processor speed’ and ‘price’. The use of matrix transformation can support a visual aspect to learning that provides both a good insight and a practical application, eg manipulating 3D models for computer games, modification of 2D images in graphic editing software.

**Synoptic assessment guidance**

Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.
The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

**P1: Demonstrate an understanding of a positional numeral system**

**Unit 2 – PO1: Understand the fundamentals of data communication**

Although understanding the value of a positional numeral system is at the heart of any unit where numbers are used to measure sizes, speeds, quantities etc, it is possible to identify specific incidences where position is key. A simple application of this by the learner could be the use of parity bits (odd or even) used in error detection and correction of data communication.

Learners should also encounter applications such as sign bits (in signed integers) or binary weights as used to describe common multiples (eg Kilobyte etc) in **Unit 1 – AO5: Demonstrate how computers process user requirements** or **Unit 7 – PO2: Understand how to secure organisational systems** where position is an important aspect for generating subnet masks for IP addresses.

**P2: Represent denary unsigned numeric integers in three different bases using correct notation**

**P3: Represent signed denary values in binary using two different techniques**

**P4: Carry out calculations involving the four common arithmetic operations using two different bases**

**Unit 1 – AO2: Understand the hardware components of a computer system**

This assessment outcome should present the learner with opportunities to explore the architecture of the computer’s internal components. Use of low level machine code or assembly by the learner may demonstrate how denary unsigned values are stored and coded in binary and hexadecimal.

Additional examination of these low level languages may practically demonstrate how typical opcodes such as ADD, SUB, MUL and DIV could be used to perform common arithmetic in these bases.

**P5: Create suitable diagrams to represent the three basic logical operations using correct notation**

**P6: Interpret a simple Boolean algebraic expression**

**Unit 1 – AO4: Understand how data is converted to information**

This unit’s assessment outcome considers the use of logical operations (such as AND, OR, NOT etc) as part of the data processing cycle. Contextualising specific data processing examples, eg online banking, can provide real world examples of logic use.

**P9: Describe different probability event types using industry examples**

**P10: Use suitable diagrams to represent two different probability events**

**P12: Gather appropriate data for an investigation of a computer related event**

**Unit 6 – PO4: Apply security measures to a network system**

This performance outcome tasks the learner with the monitoring and application of security measures present on a network. A combination of different types of logs can provide a wealth of quantitative data that may provide an ample opportunity for interpretation.
Useful links and resources

12.6 Unit 6: Network and cyber security administration

<table>
<thead>
<tr>
<th>Title</th>
<th>Network and cyber security administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>J/507/6435</td>
</tr>
<tr>
<td>Assessment</td>
<td>Externally assessed</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Resources required for this unit

Resources for this unit are varied and can be subdivided into two separate classes: research-based and practical.

For research-based activities it is likely that learners will need access to sources such as online news outlets, newspapers, magazines, books, trade journals, case studies, television documentaries etc in order to explore real life cyber attacks and their consequences. In addition anonymous samples of actual network security policies and security plans provided by industry partners would prove to be an invaluable resource. Examples of recent disaster recovery plans or industry templates would also be beneficial for learners. Information Technology Infrastructure Library (ITIL) documentation and an invited guest speaker may also prove advantageous when clarifying ITIL structure and objectives. The internet may also be used to provide models of typical penetration test procedures and reports, although much of the technical detail is often (and understandably) redacted.

Practical resources required include suitable test clients and servers (Windows and Linux, running a variety of network-based services), a quarantined network (with wired and wireless elements) and suitable forensic and penetration test suites (these typically include many of the automated tools commonly used by industry professionals and are often made available under open-source auspices); a list of these can be found in the unit content. Finally, a range of network monitoring tools and network-aware backup devices should available for learners to experience.

Synoptic assessment within this unit

IT: Cyber Security and Security Administration linked to Units 1, 2, 3, 4, 5, 7, 8 and 9.

Administering a network against cyber security threats requires a broad and deep understanding of the key concepts involved, particularly when conducting complex processes such as a penetration test (and digesting its report).

As a result, many concepts eg data, software, hardware, infrastructure, protocols, encryption and active configurations etc draw from the whole body of the programme. A signposted breakdown can be found in this unit’s synoptic assessment guidance.

Aim and purpose

This unit will allow the learner to understand network and cyber security administration. Where Unit 4 (Network threats and vulnerabilities) provides practical experience, this unit takes the concepts to the next level requiring learners to consider cyber security and the administration of network security within the context of the holistic organisational strategy.
Unit introduction
This unit focuses on the threats, defences and strategies that can be effective in securing a network.

In the cat-and-mouse game of cyber security the only real constant is change. The number of new threats is escalating as commerce becomes more reliant on the ‘Internet of things’ and network digital communication.

A cyber attack is any type of offensive manoeuvre employed by individuals or organisations that targets computer information systems, infrastructures, computer networks and/or personal computer devices. Typically, malicious acts are designed to steal, alter, or destroy a specified target by hacking into a susceptible system.

Cyber security is the ability to control access to networked systems and the information they contain. Where cyber security controls are effective, cyberspace is considered a reliable, resilient, and trustworthy digital infrastructure. However where cyber security controls are absent or poorly designed, cyberspace can be consider to be insecure.

This unit will allow a student to better understand the skills required by employers in a network and support environment.

Unit content

<table>
<thead>
<tr>
<th>Understanding the fundamentals of cyber attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification of cyber attacks</td>
</tr>
<tr>
<td>• Psychological.</td>
</tr>
<tr>
<td>• Informational.</td>
</tr>
<tr>
<td>• Structural.</td>
</tr>
<tr>
<td>Types of cyber attack</td>
</tr>
<tr>
<td>• Targeted vs untargeted.</td>
</tr>
<tr>
<td>• Commodity vs bespoke capabilities.</td>
</tr>
<tr>
<td>• Network-based attacks (DoS, DDoS) eg:</td>
</tr>
<tr>
<td>• deploying a botnet.</td>
</tr>
<tr>
<td>• Social engineering (including phishing).</td>
</tr>
<tr>
<td>• Exploiting code vulnerabilities.</td>
</tr>
<tr>
<td>• Website defacement.</td>
</tr>
<tr>
<td>• Insecure web/database applications, eg SQL injection.</td>
</tr>
<tr>
<td>• Advanced persistent threat (APT).</td>
</tr>
<tr>
<td>Perpetrators of an attack</td>
</tr>
<tr>
<td>• Cyber criminals.</td>
</tr>
<tr>
<td>• Industrial competitors.</td>
</tr>
<tr>
<td>• Government/intelligence services.</td>
</tr>
<tr>
<td>• Individual hackers.</td>
</tr>
<tr>
<td>• Hacktivists.</td>
</tr>
<tr>
<td>• Current/former employees:</td>
</tr>
<tr>
<td>• lone wolf</td>
</tr>
<tr>
<td>• contractors (genuine or fake):</td>
</tr>
<tr>
<td>• with access to system</td>
</tr>
<tr>
<td>• with access to buildings.</td>
</tr>
<tr>
<td>• Hacking groups/collectives.</td>
</tr>
<tr>
<td>• Governments (on another country – cyber warfare).</td>
</tr>
</tbody>
</table>
## Understanding the fundamentals of cyber attacks

### Targets of an attack
- Individuals.
- Organisations:
  - financial institutions
  - businesses
  - educational institutions
  - media.
- Countries/governments.

### Objectives of an attack
- Degradate, disrupt, impair or deny service.
- Compromise security/stability:
  - undermine trust
  - commercial advantage
  - financial gain, eg fraud or sale of valuable information.
- Inflict reputational/political damage:
  - promote fear, confusion, uncertainty
  - cyber terrorism.
- Economic or diplomatic advantage including:
  - paralyse financial systems
  - impede media communications
  - gather intelligence through data theft
  - national security (espionage).
- Virtual protest/political statement including:
  - agitation campaigns
  - hacktivist
  - public shaming
  - Warfare; ‘Casus belli’.

### Stages of a sophisticated attack
- Survey:
  - information acquisition
  - identify entry points (opportunities, vulnerabilities etc).
- Delivery:
  - initial compromise (infiltration)
  - establish foothold (through modified or inserted code).
- Breach:
  - escalation of privileges
  - reconnoitre of target infrastructure.
- Affect:
  - maintain presence
  - complete attack objectives (exfiltrate)
  - remove evidence of presence.

### Strategies
- Reducing exposure.
- Mitigating each stage of attack.
- Managing losses.
Controls that an organisation needs to implement to manage risks

Information security management

- Definition of risks, threats, vulnerabilities and impact.
- Loss, misuse, disclosure or damage.
- Anticipate and manage risk by planning:
  - levels of risk management:
    - strategic
    - tactical
    - operational
  - board level ownership of risks
  - communication of risks.
- Analysis of risk:
  - threat landscape
  - asset valuation and management
  - business impact of risk
  - risk analysis methodologies
  - handling risk; mitigating using countermeasures and controls
  - understanding impacts and consequences
  - security economics (altruism vs investment vs. risk).
- Codes of practice and regulatory frameworks:
  - ISO/IEC 17799: Code of Practice For Information Security Management
  - international standards, eg ISO/IEC 27000
  - regulatory, eg European GDPR and NIS directives.
### Controls that an organisation needs to implement to manage risks

<table>
<thead>
<tr>
<th><strong>Network policies</strong></th>
<th><strong>Risk management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security and operational risk management:</td>
<td>• Threat, vulnerability and risk concepts.</td>
</tr>
<tr>
<td>• Concepts and fundamentals</td>
<td>• Threat landscape.</td>
</tr>
<tr>
<td>• Types, role and function of a security policy</td>
<td>• Asset valuation and management.</td>
</tr>
<tr>
<td>• Professional roles and responsibilities</td>
<td>• Business impact of risk.</td>
</tr>
<tr>
<td>• Realising business benefit.</td>
<td>• Risk analysis methodologies.</td>
</tr>
<tr>
<td>• Types of security policies:</td>
<td>• Handling risk and selecting countermeasures and controls used to mitigate risk.</td>
</tr>
<tr>
<td>• virtual private network (VPN)</td>
<td>• Understanding impacts and consequences.</td>
</tr>
<tr>
<td>• password</td>
<td>• Security economics (altruism vs investment vs risk).</td>
</tr>
<tr>
<td>• audit</td>
<td></td>
</tr>
<tr>
<td>• acceptable encryption</td>
<td></td>
</tr>
<tr>
<td>• server security</td>
<td></td>
</tr>
<tr>
<td>• information sensitivity</td>
<td></td>
</tr>
<tr>
<td>• antivirus guidelines</td>
<td></td>
</tr>
<tr>
<td>• wireless communication</td>
<td></td>
</tr>
<tr>
<td>• risk assessment</td>
<td></td>
</tr>
<tr>
<td>• EMS network and computer acceptable use</td>
<td></td>
</tr>
<tr>
<td>• remote access</td>
<td></td>
</tr>
<tr>
<td>• acceptable use</td>
<td></td>
</tr>
<tr>
<td>• automatically forwarded email.</td>
<td></td>
</tr>
<tr>
<td>• Internal audit:</td>
<td></td>
</tr>
<tr>
<td>• understanding of process</td>
<td></td>
</tr>
<tr>
<td>• network and system equipment/inventory</td>
<td></td>
</tr>
<tr>
<td>• software licences and updates.</td>
<td></td>
</tr>
<tr>
<td>• Legislation:</td>
<td></td>
</tr>
<tr>
<td>• computer misuse</td>
<td></td>
</tr>
<tr>
<td>• data protection</td>
<td></td>
</tr>
<tr>
<td>• intellectual property and copyright</td>
<td></td>
</tr>
<tr>
<td>• regulation of security technologies</td>
<td></td>
</tr>
<tr>
<td>• employment law, legal and ethical implications.</td>
<td></td>
</tr>
<tr>
<td>• Third party management:</td>
<td></td>
</tr>
<tr>
<td>• compliance with existing policies and procedures</td>
<td></td>
</tr>
<tr>
<td>• remedy for non-compliance</td>
<td></td>
</tr>
<tr>
<td>• establishing confidence in third parties.</td>
<td></td>
</tr>
</tbody>
</table>

---

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration.
### How network security plans contribute to continuously secure systems

| Design and development considerations | • Trusted computing base (TCB).  
| | • Security architecture and patterns.  
| | • Security models and design principles; principle of least privilege, fail-safe defaults etc.  
| | • Software (program) security.  
| | • Emission security.  
| Network security plan format | • Section 1: Overview of organisation:  
| | • objectives  
| | • circulation  
| | • project team.  
| | • Section 2: Assessment results:  
| | • priorities  
| | • assets  
| | • skills and knowledge  
| | • network and systems  
| | • security  
| | • risks.  
| | • Section 3: Security plan:  
| | • action items  
| | • policy changes  
| | • user education  
| | • project timeline and responsibilities  
| | • response planning  
| | • ongoing maintenance and compliance.  
| | • Section 4: Resources and budget:  
| | • software and hardware  
| | • professional advice  
| | • internal resources.  
| Selecting and applying core technologies | • Authentication.  
| | • Access control.  
| | • Privacy controls.  
| | • Security protocols.  
| Recognising security needs across platforms | • Operating system security.  
| | • Web security.  
| | • Embedded security.  
| | • Cloud and virtualisation security.  
| | • Security as a service.  
| Cryptography | • Cipher and algorithm types.  
| | • Applications to confidentiality, integrity and authentication, public key infrastructure (PKI).  

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
### How network security plans contribute to continuously secure systems

| Network security | • Internet security protocols.  
|                  | • Tunnelling and VPNs.  
|                  | • Network attack and defence, transport layer security (TLS).  
|                  | • Human factors: usable security, psychology of security, insider threat.  
| Security systems development | • Managing secure systems development.  
|                  | • Principles of secure programming.  
|                  | • Formal approaches.  
|                  | • Understanding implementation errors and exploits.  
| Control system | • SCADA and SMART Systems.  
|                  | • Cyber system of systems (from abstract to physical effect).  
|                  | • Non-IP protocols and standards (Wi-Fi, bluetooth, GSM, CAN, MODBUS).  
|                  | • Cyber-physical systems analysis.  
|                  | • Embedded systems.  
|                  | • Assurance of control systems hardware and software.  
|                  | • Design/implementation methodologies to minimise the risk of vulnerabilities.  
|                  | • Risk modelling and risk-based decision making.  
| Continuous network security monitoring | • Plan:  
|                  | • discover  
|                  | • classify  
|                  | • define policies; what to collect; when to alert; validation; escalation  
|                  | • apply security measures; hardware, software, policies.  
|                  | • Monitor:  
|                  | • analyse  
|                  | • collect/aggregate.  
|                  | • Action:  
|                  | • escalate  
|                  | • validate.  
| Monitoring documentation | • Types of log and their purpose:  
|                  | • event logs  
|                  | • audit logs  
|                  | • security logs  
|                  | • access logs.  
|                  | • Interpreting logs to determine issues and unusual activity.  

Visit [aqa.org.uk](http://aqa.org.uk) for the most up-to-date specification, resources, support and administration.
### How network security plans contribute to continuously secure systems

| Monitoring tools | • Types of tools and their purpose:  
|                 |   • firewall, stateful packet inspection (SPI) etc  
|                 |   • intrusion detection systems (IDS); host and network based  
|                 |   • protocol analyser  
|                 |   • vulnerability scanner  
|                 |   • honeypots  
|                 |   • honeynets  
|                 |   • port scanner  
|                 |   • banner grabbing. |

### Assurance methodologies and testing

| Principles of assurance testing | • Information risk management frameworks.  
|                                | • Assessment services or standards; CHECK.  
|                                | • Management responsibilities.  
|                                | • Assessment methodologies, eg ISO/IEC 27000.  
|                                | • Understanding security vulnerabilities and related mitigation measures.  
|                                | • Testing:  
|                                |   • strategies  
|                                |   • system and software  
|                                |   • penetration  
|                                |   • TEMPTEST.  
|                                | • Security metrics.  
|                                | • Static and dynamic analysis of products and systems. |

### Operational security management and how incidents are managed

| Internet threats | • Common attacks (human and technical).  
|                 | • Malicious code.  
|                 | • Situational awareness.  
|                 | • Threat landscape and trends; top 10.  
|                 | • Computer emergency response teams (CERTs).  
|                 | • Adversarial thinking. |

| Security concerns | • Cryptography: AES and RSA, key management, digital signatures.  
|                   | • Network security: networking fundamentals, firewalls and traffic filtering, intrusion detection and prevention systems, intrusion analysis, network monitoring, mobile and wireless network security.  
|                   | • System security: authentication (secrets, tokens, biometrics), access control (MAC, DAC, RBAC) and privilege management, mobile device security and BYOD, antivirus technologies.  
|                   | • Application security: email, Web, social networks, DRM, database security, big data security, identity management.  
|                   | • Physical security: physical and environmental controls, physical protection of IT assets. |
## Operational security management and how incidents are managed

| Vulnerability assessment | • Malware analysis: static and dynamic analysis, detection techniques, host-based intrusion detection, kernel rootkits.  
|                         | • System and network-level vulnerabilities and their exploitation.  
|                         | • Vulnerability analysis and management.  
|                         | • Penetration testing.  
|                         | • Social engineering.  
|                         | • Dependable/resilient/survivable systems.  
| Intrusion detection     | • Intrusion detection methods.  
|                         | • Intrusion response.  
|                         | • Intrusion management.  
|                         | • Incident handling.  
|                         | • Intrusion analysis, monitoring and logging.  
| Investigation           | • Understanding of legislation and legal constraints.  
|                         | • Evidence gathering rules and techniques.  
| Forensics               | • Collecting, processing and preserving digital evidence.  
|                         | • Device forensics.  
|                         | • Memory forensics.  
|                         | • Network forensics.  
|                         | • Anti-forensic techniques.  
|                         | • Report writing Matrix and expert testimony.  

## The principles of disaster recovery

| Disaster recovery plan | • Budget.  
|                       | • Availability of resources: physical facilities.  
|                       | • Cost vs benefit.  
|                       | • Human constraints: people and skills.  
|                       | • Technology constraints.  
|                       | • Management’s view of risk.  
|                       | • Data.  
|                       | • Suppliers.  
| Plan                  | • Roles and responsibilities.  
|                       | • Incident response.  
|                       | • Plan initiation.  
|                       | • Procedures.  
| Sites and environments| • Hot.  
|                       | • Warm.  
|                       | • Cold.  
|                       | • Back-up generator.  

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
### The principles of disaster recovery

**Backups**
- **Types:**
  - full
  - incremental
  - differential
  - reverse delta.
- Validation.
- Frequency.
- **Media:**
  - tape
  - DVD
  - hard drive
  - solid state
  - remote
  - cloud storage.
- **Storage:**
  - working or shadow copies
  - onsite copies
  - offsite storage
  - other
  - redundant array of inexpensive/independent disks (RAID).
- Uninterruptible power supply (UPS).
- Redundancy.

### The scope, procedures and reporting processes of a penetration test

**Security audit**
- Pentest as part of a full security audit.
- Need for regular schedule.
- Role of ethical hacking.
### The scope, procedures and reporting processes of a penetration test

**Pre-engagement**

- Establish need and purpose.
- Differentiate meeting legislative or compliance needs and providing effective security.
- Defining scope of the test:
  - white box or black box
  - agree which domains, IP addresses to test
  - agree what types of test to perform
  - agree when to test:
    - inside and outside business hours
    - start and end dates, ie the agreed test period
  - agree lines of communication
  - agree secured methods of communication (including final report)
  - obtain permission to speak to third parties: hosting companies, service suppliers etc
  - agree timeline: Gantt chart etc.
- Communicate risks; potential damaging nature of some tests, possible loss or modification of data, impact on service etc.
- Agree metrics for time and costing.
- Post-compromise, agreed plan of action, ie how far to proceed.
- Obtaining formal permission to test and exemption from liabilities connected to instability or crashes.
- Deal with scope ‘creep’.
- Agree payment terms.
- Agree reporting deadline and format.
- Agree terms for retesting.

**Standards, qualifications and online resources**

- Standards:
  - penetration testing execution standard (PTES)
  - common vulnerability scoring system (CVSS).
- Qualifications:
  - certified ethical hacker (CEH)
  - licensed penetration tester (LPT)
  - certified penetration tester (CPT)
  - information assurance certification review board (IACRB).
- Online resources and advisories:
  - open web application security project (OWASP)
  - common vulnerabilities and exposures (CVE) list
  - cyber-security information sharing partnership (CiSP)
  - UK national technical authority for information assurance (CESG).
  - US national vulnerability database (NVD).
### The scope, procedures and reporting processes of a penetration test

| Types of test | • Network penetration.  
• Wireless penetration.  
• Web application.  
• Physical penetration:  
  • social engineering. |
|---------------|------------------------------------------------------------------|
| Common software tools | • Specialised operating system distributions; Kali Linux (BacktTrack), Pentoo.  
• Software frameworks and automation tools:  
  • Metasploit  
  • eEye Retina  
  • Nmap  
  • W3af  
  • Fast-Track.  
• Vulnerability scanners:  
  • Nessus  
  • OpenVAS  
  • Nexpose.  
• Password recovery tools (dictionary, brute-force or cryptanalysis, rainbow tables):  
  • Cain and Abel  
  • Rainbow Crack. |
| Specialised hardware tools | • Frequency scanner.  
• Spectrum analyser.  
• USB adaptors (802.11, GPS etc). |
| Penetration test report | • Basic principles:  
  • confidentiality  
  • avoid generic reuse of information (custom findings)  
  • document control (author, date, version etc)  
  • distribution list  
  • agreed test scope (included and excluded elements)  
  • instructions for post-pentest rollback; removal of test accounts, requested firewall or web server changes etc.  
• Business risk summary.  
• Findings:  
  • vulnerabilities and risks  
  • potential impacts  
  • suggested countermeasures  
  • other considerations.  
• Conclusion. |
The scope, procedures and reporting processes of a penetration test

Penetration test report continued

- Technical summary:
  - categories of testing (application, infrastructure etc)
  - classification of risk levels (low, medium, high) mapped to common vulnerability scoring system (CVSS)
  - application testing:
    - web server configuration
    - authentication of users
    - session management (server, cookies etc)
    - encryption
    - validation of sensitive user input (preventing XSS, SQL injection etc)
    - error handling
  - infrastructure testing:
    - configuration of devices
    - authentication of users
    - footprint reveal (version information)
    - encryption (for weak or badly applied cipher suites)
    - patching (operating system)
    - patching (tool, software libraries etc)
  - internal and external infrastructure in detail:
    - host device enumeration (hostnames, OS, IPs etc)
    - data encryption, particularly NAS drives
    - wireless networks (SSID exposure, range, encryption methods etc)
    - open ports (TCP, states and services) per IP address
    - traceroute analysis (ICMP, UDP and TCP)
    - protocol analysis (ICMP, UDP and TCP)
    - Whois information (domain registration for social engineering attacks).
- Detailed technical breakdown, per vulnerability:
  - vulnerability description
  - associated risks, affected devices, applications, pages, databases etc
  - recommendations.
- Use of references: CVSS Base, CVE-IDs, OWASP etc.
### Understanding lifecycle and service management practices to ITIL foundation

| ITIL overview | • Purpose of information technology infrastructure library (ITIL).  
|               | • Relationship to ISO/IEC20000. |
| ITIL volumes  | • Volumes that define ITIL:  
|               | • ITIL service strategy  
|               | • ITIL service design  
|               | • ITIL service transition  
|               | • ITIL service operation  
|               | • ITIL continual service improvement. |
| ITIL certification | • Levels of ITIL certification and their scope:  
|               | • foundation certificate  
|               | • practitioner’s certificate  
|               | • manager’s certificate. |

### Assessment outcomes

Unusually, there are eight assessment outcomes in this unit. Outcomes 4 and 8 are very small but are key learning areas identified by employers. They have therefore been included as separate outcomes to highlight their importance.

Learners will be able to:

#### Assessment outcome 1: Understand the fundamentals of cyber attacks

| a | Types of cyber attacks and strategies for dealing with them. |
| b | The motivations, targets and objectives of cyber attacks. |
| c | The stages of a sophisticated cyber attack. |

#### Assessment outcome 2: Understand the controls that an organisation needs to implement to manage risks

| a | Principles of information security management. |
| b | The way that codes of practice and legislative frameworks impact security measures. |
| c | The role and function of network policies and internal audits. |

#### Assessment outcome 3: Understand how network security plans contribute to continuously secure systems

| a | Design and development considerations for preparing a network security plan. |
| b | The structure and content of a network security plan. |
| c | Apply core technologies and identify security needs across platforms. |
| d | How cryptography is used to ensure confidentiality, data integrity and authentication. |
| e | Forms of network security, security systems development and control systems. |
| f | The principle and practice of continuous network security monitoring. |

#### Assessment outcome 4: Understand assurance methodologies and testing strategies

| a | Frameworks, responsibilities and methods of assurance testing. |
| b | Security vulnerabilities and appropriate testing strategies. |
Assessment outcome 5: Understand operational security management and analyse how incidents are managed

b. How security concerns are categorised, assessed and managed.
c. Legislation as it affects investigation into an intrusion and the resultant constraints.
d. Evidence gathering rules and techniques and the importance of computer forensics.

Assessment outcome 6: Understand the principles of disaster recovery

a. Disaster recovery plan, its coverage and depth.
b. Types of sites and environments used by a business.
c. Types and principles of data backup, protection and storage.

Assessment outcome 7: Understand the scope, procedures and reporting processes of a penetration test

a. Types, role and scope of a pentest.
b. Procedures and reporting processes of a pentest.
c. Standards, qualifications and online resources for pentesters.
d. Common hardware and software tools used as part of a pentest.

Assessment outcome 8: Understand the ITIL set of practices for IT service management

a. The role and function of the ITIL set of practices.
b. The scope and purpose of ITIL certification.

Assessment

This unit is assessed by an external examination set and marked by AQA.

Learners are allowed to use a non-programmable scientific calculator in the examination.

The examination consists of a written paper with two sections, A and B. Learners have to complete both sections and there are no optional questions within either section.

The exam is of 2 hours duration and the total number of marks available in the examination is 80.

Section A is worth 50 marks and consists of relatively short questions based on the whole of the specification of this unit. Learners are required to answer all the questions in Section A.

Section B is worth 30 marks and includes longer questions worth up to 15 marks each. The questions in Section B do not necessarily cover the whole specification for this unit at each assessment. Learners are required to answer all the questions in Section B.

AQA will ensure that the full content of the unit is covered equally over the life of the qualification.
Employer engagement guidance
The institution could engage with local employers and their own network staff to provide staff to
discussion networks with learners and provide work-based opportunities or cases, scenarios and
projects that learners could use for training and assessment purposes.

The British Computer Society (BCS) and the European arm of the Association for Computing Machinery,
for example, may be willing to engage with learners in discussions on networking.

Delivery guidance

General comment
Learners studying this module would benefit from having studied Unit 2 Communication technologies.

The assessment criteria could be delivered holistically rather than via discrete elements through project
work or work placement opportunities.

It would be very useful if learners could engage in work placement activities for this unit. If this is not
possible then the learner must have access to a network development or training facility in order to
carry out the design, build and testing activities that are essential elements of this unit.

IT Professionals and College partners such as JANET could provide help and resources to support this
unit.

Assessment outcome 1
Learners could carry out research in small groups, class discussions or visits to, or discussions with,
network specialists within the organisation or with external institutions to understand the fundamentals
of cyber attacks. The UK government issues statistics and information on cyber attacks annually and
would be an excellent place for learners to start their research. The National Technical Authority for
Information Assurance is GCHQ who believe that understanding the capabilities behind cyber attacks,
the vulnerabilities they exploit and how they are exploited is central to any organisation’s ability to
defend itself against them.

Assessment outcome 2
Learners could research and investigate a range of networks such as those within the institution, a local
organisation, or their own home networks and feed this back to the group in order to consolidate an
agreed understanding of information security management. From these discussions and research the
learners could, as a group, identify the policies and the security plan drivers for each network.

All of the unit content should be covered, but it is not expected that learners would have encountered
all of the elements in their investigations.

Assessment outcome 3
The most important part of deployment of network resources is planning, and it is not possible to plan
for security until a full risk assessment has been performed. Security planning involves developing
security policies and implementing controls to prevent computer risks from becoming reality. For this
assessment outcome it is important that learners (both individually and in small groups) carry out
investigation and risk assessment on different types of networks to provide the broadest experience
in different scenarios. The investigations and risk assessments will form the basis for the design of a
network security plan. Online research, surveys of local organisations, and discussions with network
professionals could also provide an insight into how a plan can be created. The results could then be
presented to the wider group and a discussion take place as to what format the plan should take.
Assessment outcome 4

Learners need to research certification and accreditation before looking at the different risk management frameworks.

In order to understand assurance methodologies and testing learners might be tasked with carrying out research on the subject individually and working in small groups to review the research undertaken. Case studies can be used to promote further discussion.

Assessment outcome 5

Operational security management again needs to be the subject of research and discussion. Learners could be divided into small groups to carry out research on, for instance, the threat landscape and present their findings to each other.

IT Professionals and College partners such as JANET could be contacted to provide help and resources to support this assessment outcome and others within unit.

Learners could also research different testing documentation and their content.

Assessment outcome 6

An understanding of the principles of disaster recovery is an important part of any security based unit. Before a DRP can be formulated risk assessment (RA) and/or business impact analysis (BIA) has to take place. For this assessment outcome learners should have access to a significant real or virtual network and information about the organisation running the network. This is so that learners can establish the organisation’s critical business activities and establish recovery time objectives (RTOs) and recovery point objectives (RPOs).

Within this outcome learners need to be given the opportunity to practice backing up data and restoring.

Furthermore, examples of redundancy need to be discussed within the context of the assessment outcome.

Assessment outcome 7

This assessment outcome can be delivered through discussion, research and practicals. The unit content lists tools that can be used to provide the learner with practical opportunities. Meanwhile the search string ‘penetration testing methodology’ will provide a range of authoritative sites for the student to research and discuss.

Assessment outcome 8

Understanding the lifecycle and service management practices to ITIL foundation certification is a key skill sought by many employers, particularly those with external customer-facing activity.

ITIL, formerly known as the Information Technology Infrastructure Library, is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. As you would expect, this is an assessment outcome that needs to be predominantly researched by the learner and discussed in the learning environment. However, with some guidance, access to case studies and access to functioning support services, the five volumes of the ITIL can be practically illustrated.
Synoptic assessment guidance

Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

<table>
<thead>
<tr>
<th>A01: Explain the fundamentals of cyber attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit 4 – PO2: Analyse security issues for a network</strong></td>
</tr>
<tr>
<td>The technical aspects underlying the threats and vulnerabilities posed by cyber attacks are examined from a network perspective in this unit’s second performance outcome; learners may benefit from being presented with a second perspective as it may enrich their understanding and ability to articulate responses when questioned on this topic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A02: Explain the controls that an organisation needs to implement to manage risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit 2 – AO2: Understand the fundamentals of computer networks</strong></td>
</tr>
<tr>
<td>The underlying concept of risks associated with networking that an organisation might face are introduced in this unit’s second assessment outcome and forms a sound foundation that the learner should build upon to explore this topic in greater depth.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A03: Explore how network security plans contribute to continuously secure systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit 3 – PO4: Design and build a network from a specification</strong></td>
</tr>
<tr>
<td>Security should be considered an integral aspect of any network design. This unit’s fourth performance outcome introduces the concept of network planning, forming the basis for any subsequent network security plan.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A06: Explain the principles of disaster recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit 4 – PO5: Plan for business continuity to mitigate risks and impact on organisations caused by insecure networks</strong></td>
</tr>
<tr>
<td>Disaster recovery is examined in unit 6 from an administrative perspective. Unit 4’s examination of business continuity attempts to follow a more practical path, examining the role of a disaster recovery plan as part of a much bigger process, that of keeping the organisation functioning in the event of a network impact. Learners may choose to make these links to strengthen their understanding of the business continuity process.</td>
</tr>
</tbody>
</table>
A07: Explain the scope, procedures and reporting processes of a penetration test

The scope of a penetration test is typically extensive, covering many different aspects such as data, software, hardware, infrastructure, protocols, encryption and active configurations. Many of these are covered conceptually throughout many units in the programme. Learners should establish a firm grasp of these concepts before tackling the intricacies of a penetration test.

Key underpinning penetration test concepts can be drawn from the following linked outcomes.

For data, software and hardware:
Unit 1 – AO1: Understand the different types of computer
Unit 1 – AO3: Understand the software requirements of a computer system
Unit 1 – AO5: Demonstrate how computers process user requirements
Unit 5 – PO1: Work with number systems

For infrastructure and protocols:
Unit 2 – AO5: Understand network conceptual models, protocols and devices
Unit 3 – PO2: Identify the different types of network architectures and technology types

For encryption and active configuration:
Unit 4 – PO1: Understand network security testing
Unit 4 – PO2: Analyse security issues for a network
Unit 4 – PO3: Deploy secure networks
Unit 4 – PO4: Apply security settings to network technologies
Unit 7 – PO1: Select hardware and software to promote security for a network system
Unit 7 – PO2: Understand how to secure organisational systems
Unit 7 – PO3: Understand legal issues and standards affecting security
Unit 7 – PO4: Assure controls to ensure data integrity and security
Unit 7 – PO5: Implement access controls to manage identity
Unit 8 – PO4: Recognise vulnerabilities and counter threats to website and mobile technologies
Unit 8 – PO5: Demonstrate the key features and functions of operating system shell scripting
Unit 8 – PO6: Recognise the key features and functions of data security and encryption
Unit 9 – PO1: Understand the principles of computer forensic investigation

Useful links and resources

Books

Websites
• Computer Emergency Response Team (CERT): cert.gov.uk
• CESG (the information security arm of GCHQ and the National Technical Authority for Information Assurance in the UK): cesg.gov.uk/Pages/homepage.aspx
• Cisco: cisco.com
• JANET network CSIRT: jisc.ac.uk/csirt
• PuTTY: chiark.greenend.org.uk/~sgtatham/putty/download.html
• Search Mobile Computing: searchmobilecomputing.techtarget.com
• Serial Communication: learn.sparkfun.com/tutorials/serial-communication/rules-of-serial
• The OSI Model’s Seven Layers: support.microsoft.com/kb/103884
• Wireshark Protocol Analyser: wireshark.org/download.html
12.7  Unit 7: Managing identity and access to systems

<table>
<thead>
<tr>
<th>Title</th>
<th>Managing identity and access to systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>Y/507/6438</td>
</tr>
<tr>
<td>Unit assessment type</td>
<td>Centre assessed and externally quality assured</td>
</tr>
<tr>
<td>Recommended assessment method</td>
<td>Practical assignment</td>
</tr>
<tr>
<td></td>
<td>This is the preferred assessment method for this unit. A centre may choose an alternative method of assessment, but will be asked to justify this as part of the quality assurance process.</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>Problem-solving 6</td>
</tr>
<tr>
<td>Resources required for this unit</td>
<td>The resources/equipment that will be required to deliver the unit include:</td>
</tr>
<tr>
<td></td>
<td>Windows PC, Linux, Apple Macintosh OS X or other suitable platforms that provide the learner with access to the software tools and configuration options necessary to demonstrate required skills such as creating access control lists and performing various encryption techniques.</td>
</tr>
<tr>
<td></td>
<td>Many tools are available via open source options that help to keep costs low in terms of delivery. The promotion of Linux-based solutions (physical or virtual) also offer a wealth of command-line utilities and opportunities for kinaesthetic learning and help to more accurately reflect the type of tools used in the sector.</td>
</tr>
<tr>
<td>Synoptic assessment within this unit</td>
<td>IT: Cyber Security and Security Administration linked to Units 1, 2, 3, 4, 5 and 6.</td>
</tr>
<tr>
<td></td>
<td>Draws particularly on Unit 1 for the underlying principles of data, how it is encoded and stored in RAM and on backing storage devices. It also introduces the learner to the concept of authentication, a core concern when attempting to manage a user's identity and access to systems.</td>
</tr>
<tr>
<td></td>
<td>Unit 2 describes how data is encoded for communication over different transmission media. Unit 3 provides the learner with an understanding of access control lists (ACLs) from a networking perspective.</td>
</tr>
<tr>
<td></td>
<td>Unit 4 includes additional coverage of network security concepts such as wireless encryption and email filtering.</td>
</tr>
<tr>
<td></td>
<td>Unit 6 complements this unit with cover (from an administration perspective) on cloud storage, authentication, codes of practice and regulatory frameworks.</td>
</tr>
<tr>
<td></td>
<td>A signposted breakdown can be found in this unit's synoptic assessment guidance.</td>
</tr>
</tbody>
</table>

6 Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.
Aim and purpose
To equip learners with the necessary knowledge and practical ability to protect organisational systems and their sensitive data through the application of best practice logical and physical security measures that attempt to meet legislative needs while remaining within an ethical framework.

Unit introduction
Most modern businesses store critical data electronically, permitting individuals access to them via robust networked solutions, controlled through the twin concepts of authentication and authorisation. Modern cyber attacks often take advantage of poor planning, weak security and ineffective identity management to wreak havoc and potentially endanger systems and individuals.

In this unit learners will discover not just how to store data safely on a network but how to apply appropriate logical and physical security methods to deter direct attacks, intrusion attempts and unauthorised data extraction and amendment. Care is also taken to ensure that learners are aware of the legal issues (and consequences) surrounding data security and the crucial role of information security management standards in specifying and encouraging best practice across all sectors that use IT. In addition time is spent ensuring that data integrity is upheld and that access control and management of identity conform to the most stringent controls available.

Given the ubiquitous nature of sensitive data in the modern world, any IT professional, particularly one pursuing a career in Cyber Security, should be well-versed in these concepts.

Unit content

<table>
<thead>
<tr>
<th>Hardware and software to promote security for a network system</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intrusion detection and prevention systems</strong></td>
</tr>
<tr>
<td>• Firewall; stateful packet inspection (SPI) etc.</td>
</tr>
<tr>
<td>• Intrusion detection systems (IDS); host and network based:</td>
</tr>
<tr>
<td>• behaviour based</td>
</tr>
<tr>
<td>• signature based</td>
</tr>
<tr>
<td>• anomaly based</td>
</tr>
<tr>
<td>• heuristic.</td>
</tr>
<tr>
<td>• Virus protection.</td>
</tr>
<tr>
<td>• Spyware protection.</td>
</tr>
<tr>
<td>• File and folder monitoring.</td>
</tr>
<tr>
<td>• Alarms.</td>
</tr>
<tr>
<td>• Honeypots.</td>
</tr>
</tbody>
</table>
Hardware and software to promote security for a network system

Cryptography algorithms and protocols

- Theory of cryptography:
  - plaintext
  - encryption key
  - ciphertext.
- Block vs stream encryption methods.
- Hashing versus one-way encryption.
- Key escrow.
- Steganography.
- Symmetric encryption and weaknesses.
- Asymmetric encryption; key pairs – public and private.
- Data integrity algorithms, eg hashing, checksums (MD5, SHA) etc.
- Authentication protocols.
- Relative strength of encryption methods (strong vs. weak).
- Common cryptographic methods, eg:
  - triple data encryption standard (DES)
  - RSA
  - Blowfish
  - Twofish
  - advanced encryption standard (AES).
- Use of encryption algorithms and protocols during ‘data in motion’, ie transmission or transfer, eg:
  - secure sockets layer (SSL)
  - transport layer security (TLS)
  - secure shell (SSH)
  - hypertext transfer protocol secure (HTTPS).

Access control (eg)

- Biometrics; types.
- Passwords; strength levels and good practice (reuse, expiration etc).
- User permissions.
- Digital signatures and certificates; Public Key Infrastructure (PKI).
- Protocols.
- Logins.
- Logging, shared access.
## Hardware and software to promote security for a network system

<table>
<thead>
<tr>
<th>Wireless security features</th>
<th>(eg)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Security weaknesses and attacks against each:</td>
</tr>
<tr>
<td></td>
<td>• service set identification (SSID) broadcast</td>
</tr>
<tr>
<td></td>
<td>• wired equivalent privacy (WEP)</td>
</tr>
<tr>
<td></td>
<td>• Wi-Fi Protected Access (WPA)</td>
</tr>
<tr>
<td></td>
<td>• Wi-Fi Protected Access II (WPA2).</td>
</tr>
<tr>
<td></td>
<td>• Associated WPA technologies and implementations:</td>
</tr>
<tr>
<td></td>
<td>• pre-shared key (PSK)</td>
</tr>
<tr>
<td></td>
<td>• advanced encryption standard (AES)</td>
</tr>
<tr>
<td></td>
<td>• temporal key integrity protocol (TKIP)</td>
</tr>
<tr>
<td></td>
<td>• CCMP (counter cipher mode with block chaining message authentication code protocol)</td>
</tr>
<tr>
<td></td>
<td>• extensible authentication protocol (EAP)</td>
</tr>
<tr>
<td></td>
<td>• lightweight extensible authentication protocol (LEAP)</td>
</tr>
<tr>
<td></td>
<td>• protected extensible authentication protocol (PEAP).</td>
</tr>
<tr>
<td></td>
<td>• MAC association and filter.</td>
</tr>
<tr>
<td></td>
<td>• Antenna placement and types.</td>
</tr>
<tr>
<td></td>
<td>• Power level controls.</td>
</tr>
</tbody>
</table>

| Email security features | • Spam filters. |
|                        | • Email encryption plug-ins. |
|                        | • Attachment scanners. |
|                        | • Email scanners. |
### Securing organisational systems

#### Physical security
- Environmental controls, eg:
  - fire suppression
  - Heating, Ventilating and Air Conditioning (HVAC)
  - temperature and humidity controls
  - Electromagnetic Interference (EMI) shielding.
- Physical measures, eg:
  - doors
  - locks
  - three-barrier system
  - mantraps
  - guards
  - signs
  - safe
  - locked cabinets
  - motion detection.
- Data screening:
  - cable shielding (types; cores, foil and braid).
- Procedural measures, eg:
  - signing in/out procedures
  - visitor passes
  - access to areas
  - employee training
  - code of conduct:
    - A list of expected behaviours that employees sign to confirm their intended compliance
    - computer misuse agreement.
- Electronic methods, eg:
  - smart cards
  - two-factor authentication hardware “token”, eg RSA SecurID
  - biometrics, eg:
    - iris/retinal scan
    - finger print scan
    - voice recognition
    - keystroke behaviour
    - pros and cons of different biometric authentication methods
  - surveillance, ie closed-circuit TV
  - activity logging.
## Securing organisational systems

### Software and network security
- Encryption techniques public and private.
- Virtual Private Networks (VPNs).
- Data encryption.
- Passwords.
- Access levels.
- Software updates.
- Firewalls.
- Web security gateways.
- Proxy servers.
- Antivirus.
- Anti-Spyware.
- Copyright.
- Software licensing, eg:
  - open source
  - shareware and freeware
  - commercial software.

### Hardening methods
- Common hardening benchmarks.
- Operating system:
  - hotfixes
  - service packs.
- Applications and firmware:
  - patches
  - updates.
- Server and client:
  - pack management
  - group policies.

### Authentication methods
- One, two and three-factor authentication.
- Single sign-on.
- Password updating.
- Password strength.
## Legal issues and standards affecting security

| Codes of conduct and contract clauses | • Formal agreements, eg:  
| | • non-disclosure  
| | • unauthorised use of external media  
| | • unauthorised use of computers for private activities such as buying goods online  
| | • installation of unauthorised software  
| | • use of social media at work  
| | • use of email  
| | • removal of company data.  
| | • Risk reduction policies, eg:  
| | • security policy  
| | • mandatory holidays/breaks  
| | • job rotation  
| | • separation of duties  
| | • least privilege.  
| Legislation | • Purposes, eg:  
| | • protect data about people  
| | • hacking of computer systems, services and data  
| | • protecting copyright and patents  
| | • censorship of the internet  
| | • health and safety.  
| | • Legal liability, eg Data Protection Act (1998):  
| | • criminal offences  
| | • fines  
| | • enforcement notice  
| | • personal liability.  
| | • Legislation, eg:  
| | • *Computer Misuse Act* (1990)  
| | • *Communications Act* (2003)  
| | • *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulation* (2000)  
| | • *Data Protection Act* (1998)  
| | • *Privacy and Electronic Communications (EC Directive) Regulations (2003) and Amendment to the regulation* (2011)  
| | • *Data Retention (EC Directive) Regulations* (2009)  
| | • *Copyrights, designs and patents* (1988)  

### Legal issues and standards affecting security

#### Ethical factors
- **Issues:**
  - privacy
  - accuracy
  - property
  - accessibility.
  - Freedom of information vs personal privacy.
  - Copyright, permission to use; eg images CCTV footage.

#### Bodies
- ISO (International Organization for Standardization).
- IEC (International Electrotechnical Commission).

#### ISO 27000 family
- **Purpose** – managing security of assets such as:
  - financial information
  - intellectual property
  - employee details
  - sensitive information entrusted by third parties.

#### ISO/IEC 27001
- **Scope.**
- **Sections:**
  - context of the organisation
  - leadership
  - planning
  - support
  - operation
  - performance evaluation
  - improvement.

### Controls to promote data integrity and security

#### Cloud storage
- **What is cloud storage?**
- **Cloud storage types:**
  - using network attached storage (NAS); technology and features
  - using storage area network (SAN); technology and features
  - NAS/SAN performance comparison.

#### Big Data
- **Definition and examples.**
- **Handling.**

#### Digital data states
- **Classification of data as being in one of three digital states:**
  - data at rest: stored in digital form, eg database, spreadsheet stored on physical media (disks, tapes, USB)
  - data in use: being processed by computer system’s CPU (central processing unit)
  - data in motion: data being transmitted between source and destination, often over a network.
- Preferred methods used to protect data in different digital states, eg encryption methods such as AES, SHA-256 etc.
## Controls to promote data integrity and security

| Hardware based encryption devices | • Types:  
| | • Hardware security module (HSM); secure device that manages digital keys, typically for a network or a computer  
| | • Trusted platform module (TPM); secure cryptoprocessor integrated into hardware  
| | • encrypted media, eg hard disk, USB.  
| Encryption software | • ‘On-the-fly’ encryption (OTFE) methods:  
| | • Bitlocker  
| | • TrueCrypt  
| | • CipherShed  
| | • Pretty Good Privacy (PGP).  
| Permissions and Access Control Lists | • Types of access control lists, eg:  
| | • file systems (read, write, modify, execute permissions etc)  
| | • networking (IP addresses, port numbers permissions)  
| | • relational database systems (Data Control Language, GRANT, REVOKE etc).  
| Data policies | • Data policies affecting data at different life stages:  
| | • wiping/erasure  
| | • disposing  
| | • retention  
| | • storage.  

## Access control and identity management

| Discrete stages of access control | • Three discrete stages/concepts:  
| | • identification, eg keying username  
| | • authentication, eg keying correct password or presenting a token or smart card  
| | • authorisation, eg occurs after successful authentication, defining what exactly the user can do.  
| Common authentication services (eg) | • Lightweight Directory Access Protocol (LDAP).  
| | • Kerberos protocol.  
| | • Remote Authentication Dial In User Service (RADIUS) protocol.  
| | • Diameter protocol.  
| | • Terminal Access Controller Access-Control System (TACACS+) protocol.  
| | • Extended TACACS (XTACACS) protocol.  
| | • Security Assertion Markup Language (SAML).  

Access control and identity management

Common authentication methods

- Tokens (hardware, software etc) and types:
  - static password
  - synchronous dynamic password
  - asynchronous password
  - challenge response.
- Cards:
  - CAC (Common access card – primarily US)
  - smart card.
- Multifactor authentication.
- Password algorithms:
  - Time-based One-time Password Algorithm (TOTP)
  - HMAC-based One Time Password (HOTP).
- Protocols:
  - Password Authentication Protocol (PAP)
- Single sign-on (SSO).
- Access control.
- Implicit deny.
- Trusted OS.
- Advantages and disadvantages of different authentication methods, eg SSO:
  - pros – reduces time spent re-entering passwords for multiple con –
    services, even after being authenticated
  - cons – it can make authorisation more problematic.

Authentication factors

- Factors for authentication:
  - identity/role – something you are
  - possession – something you have
  - knowledge – something you know
  - location – somewhere you are
  - action – something you do.

Identification

- Biometrics.
- Personal identification.
- Verification card.
- Username.

Federation

- Federated ID.
- Federated Identity Systems, eg OpenID.
- Federated logins, eg Facebook, Google.
- OpenID vs OAuth.

Transitive trust/ authentication

- Two-way relationship created between parent and child domain.
Performance outcomes
On successful completion of this unit, learners will be able to:

<table>
<thead>
<tr>
<th>Performance outcome 1:</th>
<th>Select hardware and software to promote security for a network system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance outcome 2:</td>
<td>Understand how to secure organisational systems.</td>
</tr>
<tr>
<td>Performance outcome 3:</td>
<td>Understand legal issues and standards affecting security.</td>
</tr>
<tr>
<td>Performance outcome 4:</td>
<td>Assure controls to ensure data integrity and security.</td>
</tr>
<tr>
<td>Performance outcome 5:</td>
<td>Implement access controls to manage identity.</td>
</tr>
</tbody>
</table>

Grading criteria

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO1: Select hardware and software to promote security for a network system</strong></td>
<td>The achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td><strong>P1</strong></td>
<td>Identify five intrusion detection systems and explain why they would be required to secure a selected networked system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P2</strong></td>
<td>Use four access control methods that would be required to secure a network system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P3</strong></td>
<td>Implement two wireless security features and two email security features to secure a network system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO2: Understand how to secure organisational systems</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P4</strong></td>
<td>Explain how physical security measures could reduce the risk of damage in a given system providing at least six examples.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Performance outcomes

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The achieve a pass the learner must evidence that they can:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P5</strong> Explain how software security measures could reduce the risk of damage in a given system providing at least six examples.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M2</strong> Discuss the operation and use of an encryption technique to ensure security of information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P6</strong> Plan suitable measures to secure a given computer system, <strong>implement</strong> them and <strong>review</strong> their effectiveness in <strong>solving</strong> the security <strong>problems</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P7</strong> Explain how authentication methods secure organisational systems.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M3</strong> Discuss how a computer system and its data could be made secure from <strong>three</strong> potential threats by using a VPN.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D1</strong> Consider how hardening can benefit a selected system by developing a comprehensive technical group security policy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P8</strong> Create codes of conduct to protect a given organisational system by selecting relevant legislative requirements, standards and ethical factors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M4</strong> Discuss the commercial and reputational damage that can be caused by an employee breaching the company’s IT codes of conduct.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D2</strong> Evaluate the potential conflict between the Freedom of Information Act and personal privacy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P9</strong> Explain the need for information security management frameworks.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M5</strong> Describe the scope of the ISO27000 family including <strong>four</strong> key questions that an organisation should answer to demonstrate ISO/IEC270001 compliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PO3: Understand legal issues and standards affecting security**

- **P8** Create codes of conduct to protect a given organisational system by selecting relevant legislative requirements, standards and ethical factors.
- **M4** Discuss the commercial and reputational damage that can be caused by an employee breaching the company’s IT codes of conduct.
- **D2** Evaluate the potential conflict between the Freedom of Information Act and personal privacy.
<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO4: Assure controls to ensure data integrity and security</strong></td>
<td>The achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td><strong>P10</strong> Explain cloud storage for big data and compare two available methods.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P11</strong> Describe and demonstrate the three different digital states of data.</td>
<td><strong>M6</strong> Select, justify and demonstrate preferred methods used to protect data in each of the three different digital states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P12</strong> Describe two hardware based encryption devices.</td>
<td><strong>M7</strong> Demonstrate the use of two ‘on the fly’ encryption methods.</td>
<td><strong>D3</strong> Compare and contrast two ‘on the fly’ encryption methods.</td>
<td></td>
</tr>
<tr>
<td><strong>P13</strong> Demonstrate the use of two different types of access control lists which control access to data.</td>
<td><strong>M8</strong> Compose sample policies that affect data at two different lifestages for a commercial scenario.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PO5: Implement access controls to manage identity</strong></td>
<td><strong>P14</strong> Differentiate the three stages of access control.</td>
<td><strong>M9</strong> Demonstrate the use of three different common authentication services.</td>
<td><strong>D4</strong> Evaluate four different common authentication methods.</td>
</tr>
<tr>
<td><strong>P15</strong> Describe five different authentication factors.</td>
<td><strong>M10</strong> Demonstrate an example of identification, federation and transitive trust.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assessment amplification**

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

There is no mandatory division of grading criteria although, as can be seen from the Grading criteria grid, some are naturally linked either by learning outcome or by a developmental theme. Connections between the various pass, merit and distinction criteria can therefore suggest logical assessment grouping but do not necessarily have to be followed.
Finding a single real world scenario that can cover all criteria is difficult, but not impossible. For example, a local employer seeking ISO/IEC 27001 compliance may be a useful ally in terms of sourcing anonymised case studies. The key to assessment in this unit, as in others, is to make assessment a natural outcome of the learning experience, with skills being assessed at a level appropriate to the learner’s level of experience.

Integrative assessments that connect this unit to others via connected tasks are also encouraged and it is possible that evidence produced during work for this unit may be used to provide evidence for criteria in other units.

As with all units, in order to gain a pass grade, learners must generate evidence that meets all listed pass criteria.

For P6 learners should record the processes undertaken so that these can be checked by the assessor. Learners could, for example, create a checklist of the steps they will undertake and sign each step when completed. It is important that the full problem-solving cycle can be demonstrated by the learner, i.e. plan, do and review.

To achieve M4 and D2 learners should ideally source selected real world case studies and examples to lend authenticity to their arguments and findings.

M6 tasks the learners with firstly identifying the three digital states of data and then selecting, justifying and demonstrating how to protect data in each of these states. Learners should explain why the method they are using is the most appropriate for the data state, ideally supporting their arguments with third-party evidence or research.

M7 requires the learners to practically use two ‘OTFE’ methods and evidence their success. The demonstration, as with others, may be recorded using any viable technique (or combination), e.g. video, photographs, screen captures etc. M9 and M10 require similar practical demonstrations.

M8 asks the learners to write two policy documents that affect the way data is organisationally dealt with at different stages of its life. At this level learners should reference best practice as part of their policy guidance and it must relate to a commercially relevant application or process.

For D3 learners should identify two ‘OTFE’ methods and research their similarities and differences, ideally referencing industry usage and preferences.

D4 requires a detailed examination of four different authentication methods, preferably ones used popularly in industry. This should examine their relative strengths, weaknesses and overall effectiveness. Commercial examples of usage should be included to support the learner’s evaluation.

As with all units, in order to secure a merit, learners must achieve all of the pass criteria listed, and all of the merit criteria. Distinction can only be awarded if all grading criteria (pass, merit and distinction) are achieved.

**Employer engagement guidance**

Where possible set problems encountered by the learner should have a strong vocational context; engaging with local SMEs (small and medium-sized enterprises) can provide a rich source of real world scenarios to investigate and solve.

A range of organisations exist that may help centres engage local employers in the delivery and potential assessment of this unit, for example The Tech-Partnership (thetechpartnership.com).
Delivery guidance

General comment
Many of the concepts in this unit complement topics taught in other units and offer many opportunities for synergy of delivery and synoptic assessment, both formative and summative. As such, although it is suggested that the content is delivered to follow the order of the learning outcomes in this unit specification, it is not the only sequence that could be used and tutors are encouraged to consider the holistic nature of the learner’s programme and the scheme itself.

Learners must have access to the hardware and software facilities necessary for the opportunity to generate evidence for all of the grading criteria listed; As such, if centres cannot guarantee these resources, the unit should not be attempted.

Many aspects of this unit require learners to deliver precise written or oral content (via presentation or viva) with many technical aspects that they may find challenging, particularly if real world exposure to such concepts is low. Where possible it is suggested that the content is taught through worked case studies, particularly involving guest speakers or industry professionals who can offer ‘day in the life’ style insight of working in the information security industry.

Performance outcome 1
Learners should be taught about the different hardware and software tools available to promote network security. It is important that learners have access to as many different tools as possible so that they can see how they actually work on a system and their purpose in securing the network. Learners could continue to work in their small groups and select appropriate hardware and software to address the security issues that they had identified previously. They could then retest the system to ensure that the issues have been addressed.

Performance outcome 2
Learners need to be aware of a range of physical security measures and software applications and techniques used to secure data and how they work. They should understand that security can be both logical and physical and should assess the benefits and drawbacks of both in context.

Practical experience using a range of software tools, where possible, is invaluable. Learners will need to practice configuring software such as antivirus, firewalls, VPNs, software updates and encrypt data in order to secure a system.

Performance outcome 3
Learners should have access to, or could research, a range of organisational codes of conduct. They need to understand how each code affects security and its importance in maintaining it.

Discussions around ethics, considerations and implications at this point can highlight potential issues that security professionals may encounter in the workplace.

Critical focus is also placed on information security management and the value, reassurance and recognition that bodies place in frameworks and standards such as ISO 27001:2013; learners must appreciate the importance of these. They should understand the scope of the standards and their purpose in specifying best practice, measuring and evaluating an organisation’s information security management systems.
Performance outcome 4
In order for learners to manage information security effectively they should be made aware of different digital states and how best to protect data in each of these using the most appropriate software and hardware solutions.

Performance outcome 5
The final outcome focuses on authentication and the modern techniques used to establish the authenticity of a user, both in terms of identity and knowledge. Additional attention is placed on network related techniques such as domain-based transitive trust and federation between online services.

Synoptic assessment guidance
Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

**P1: Identify five intrusion detection systems and explain why they would be required to secure a selected networked system**

Unit 3 – PO5: Undertake end user network testing
Unit 4 – PO1: Understand network security testing
Unit 4 – PO3: Deploy secure networks
Unit 6 – AO3: Explore how network security plans contribute to continuously secure systems

These units and their outcomes offer alternative perspectives for the learner regarding the scope and use of different intrusion detection and prevention systems. In Unit 3 the focus is on IDS as an end user testing tool of a newly designed network; for Unit 4 it is explored specifically for testing security and deployment. Unit 6 examines how IDS may be used to monitor network activity in a bid to keep the network secure.

**P3: Implement two wireless security features and two email security features to secure a network system**

Unit 3 – PO2: Identify the different types of network architectures and technology types
Unit 4 – PO1: Understand network security testing
Unit 4 – PO2: Analyse security issues for a network

Concepts such as encryption to protect wireless networks and spam filters to isolate and remove suspect email are discussed in these units, mainly from an implementation, cracking or functionality perspective. Learners may be able to amplify their answers by drawing practical skills and knowledge delivered through this coverage in order to complete this grading criterion.
P5: Explain how software security measures could reduce the risk of damage in a given system providing at least six examples

Unit 1 – AO3: Understand the software requirements of a computer system
The learner is introduced to many of these software security measures in this unit and this should provide a sound platform for learners to tackle this grading criterion.

Unit 4 – PO1: Understand network security testing
Unit 4 – PO2: Analyse security issues for a network
Unit 4 – PO4: Apply security settings to network technologies
This unit has multiple instances where different software measures are tested, analysed and configured for use. A practical unit, this should provide ample examples for the learner to reference when completing this grading criterion.

Unit 6 – AO5: Explain operational security management and analyse how incidents are managed
Many of the software-based security measures used to reduce system damage are examined as part of the day-to-day administrative responsibilities on a network.

P7: Explain how authentication methods secure organisational systems

Unit 1 – AO3: Understand the software requirements of a computer system
The concept of authentication is introduced in this unit’s third assessment outcome as a form of security software. This should provide a firm foundation for learners to build upon when tackling this criterion.

Unit 4 – PO1: Understand network security testing
Authentication of users is a key aspect when testing the security of hosts that are connected to a network. It is likely that a standard network login will only reflect a one-factor authentication method (also referred to as ‘what you know’). Fortuitously this can be used both as a practical demonstration to support the learner’s understanding and to highlight the weakness of this limited (but popular) approach.

Unit 6 – AO3: Explore how network security plans contribute to continuously secure systems
Authentication and its deployment is a core technology that can be used as part of a security plan to keep networked systems secure. Learners may benefit from understanding its importance in such plans and be able to advise more confidently if they can describe the different levels of authentication (one, two, three etc) available.

P8: Create codes of conduct to protect a given organisational system by selecting relevant legislative requirements, standards and ethical factors

Unit 6 – AO2: Explain the controls that an organisation needs to implement to manage risks
This unit’s assessment outcome specifically focuses on the codes of practice and legislation that may be leveraged to inform the network policies used to manage risks in an organisation. This additional viewpoint may provide the learner with a deeper understanding of what should be protected and how a sensible – and fair – code of conduct can be created.

P9: Explain the need for information security management frameworks

Unit 6 – AO2: Explain the controls that an organisation needs to implement to manage risks
This unit’s assessment outcome introduces the idea of codes of practice and regulatory frameworks that inform modern information security management. Learners could use this as a reference point when satisfying the demands of this grading criterion.
P10: Explain cloud storage for big data and compare two available methods

Unit 6 – AO6: Explain the principles of disaster recovery
Cloud storage features as a backup destination as part of an organisation's disaster recovery plans. Learners should benefit from being familiar with the technology, its core concepts and options before tackling this grading criterion.

P11: Describe and demonstrate the three different digital states of data

Unit 1 – AO2: Understand the hardware requirements of a computer system
Unit 1 – AO5: Demonstrate how computers process user requirements
These two assessment outcomes introduce the concept of data and how it is stored inside a computer in different digital states, both ‘at rest’ (i.e. stored in a physical media) and ‘in use’ (when being processed by the computer system’s CPU). In addition they discuss data storage units and character encoding – both key aspects that the user should grasp firmly before attempting this grading criterion.

Unit 2 – AO1: Understand the fundamentals of data communication
Learners will undoubtedly benefit from understanding how data is electronically communicated between two points as this reflects the final digital state, ‘data in motion’.

P12: Describe two hardware based encryption devices

Unit 1 – AO1: Understand the different types of computer
Unit 2 – AO2: Understand the hardware requirements of a computer system
Hardware based encryption devices are essentially examples of a single purpose computer systems – a specialist device dedicated to encrypting and decrypting data. It is likely therefore that learners will be able to identify its components and discuss its functionality through learning covered in these two introductory assessment outcomes.

P13: Demonstrate the use of two different types of access control lists which control access to data
P14: Differentiate the three stages of access control

Unit 3 – PO 2: Identify the different types of network architectures and technology types
The concept of access control lists (ACLs) is introduced in this unit’s second performance outcome. Learners will initially encounter ACLs as contributing to a network’s basic security, giving them a sound foundation to tackle this grading criterion.

P15: Describe five different authentication factors

Unit 1 – AO3: Understand the software requirements of a computer system
The concept of authentication is introduced in this unit’s third assessment outcome as a form of security software. This should provide a firm foundation for learners to build upon when tackling this criterion.

Unit 4 – PO1: Understand network security testing
Authentication of users is a key aspect when testing the security of hosts that are connected to a network. It is likely that a standard network login will only reflect a one-factor authentication method (also referred to as ‘what you know’). This can be used both as a practical demonstration to support the learner’s understanding and to highlight the weakness of this limited (but popular) approach.

Unit 6 – AO3: Explore how network security plans contribute to continuously secure systems
Authentication and its deployment is a core technology that can be used as part of a security plan to keep networked systems secure. Learners may benefit from understanding its importance in such plans and be able to advise more confidently if they can describe the different levels of authentication (one, two, three etc) available.
Useful links and resources

Books


Websites

- Authentication World: [authenticationworld.com](http://authenticationworld.com)
- TechTarget SearchSecurity: [searchsecurity.techtarget.com](http://searchsecurity.techtarget.com)
### 12.8 Unit 8: Programming for networking and security (optional)

<table>
<thead>
<tr>
<th>Title</th>
<th>Programming for networking and security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>D/507/6439</td>
</tr>
<tr>
<td>Assessment</td>
<td>Internally assessed and externally verified</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s) contextualised within this unit</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Resources required for this unit**

Suitable Windows PC, Linux, Apple Macintosh OS X, Apple iOS or other suitable platforms, which offer Integrated Development Environments suited to learning and exploring the various programming technologies here.

These include, but are not limited to: Microsoft ASP.net, PHP, Java, JavaScript, a web browser, syntax highlighted text editors, database server (eg MySQL) and web server software such as Apache or IIS.

In addition some aspects of the unit will require user rights on the development and target platforms to compile programs and install executable code. Firewalls may also have to be configured to permit data transfers on selected protocols (eg FTP, SSH) between the server and its clients. Access to the command line/shell of an operating system in order to write scripts.

Learners should also have access to suitable offline and online learning material, manuals, help sheets and coded examples in order to encourage self-sufficiency.

**Synoptic assessment within this unit**

IT: Cyber Security and Security Administration linked to Units 1, 3, 4, 5, 6 and 7.

Unit 1 provides the learner with a solid grounding in the different types of software and hardware that are likely to form part of a website technology solution. In addition this unit also introduces the concept of programming languages and relational database systems which, when combined, form powerful website solutions.

Unit 3 focuses on developing and maintaining computer networks. A significant part of any network development includes the configuration of wireless networks.

Unit 4 has specific links to vulnerabilities linked to web server and database services, often created by poorly written program code.

Unit 5 gives the learner the opportunity to sharpen their mathematical skills, proving essential for learners when tackling the logic, arithmetic and algorithms needed to get the very best out of website technologies.

Units 6 and 7 support the learner when working practically with encrypted data by providing detailed background on the different cipher suites available and how they work.

A signposted breakdown can be found in this unit’s synoptic assessment guidance.
Aim and purpose
There is agreement that network engineers and security professionals should have a working understanding of computer programming as system vulnerabilities are often caused by poor coding practice. This unit firstly focuses on the basics of programming. In addition, learners will explore client- and server-side scripting using JavaScript or similar. This will help equip learners with the knowledge to understand the vulnerabilities of (and threats to) software, websites and mobile devices and also give them the practical ability to create scripts for the client and server-sides of websites and operating systems.

Unit introduction
As the platforms and devices available on which to distribute software have increased, so has the awareness of network managers/engineers of their need to understand the threats posed to them by the vulnerabilities in code and scripts.

In this unit learners will gain an understanding of how programming works at a fundamental level in order for them to be able to create their own scripts, for operating systems and for both client and server-side use; create useful batch-type programs to help manage networks and see how vulnerabilities and threats to programs and scripts can be determined even at the design stage and that they should all be built with security as a core part of the script itself rather than as an afterthought.

Unit content

<table>
<thead>
<tr>
<th>The tools, features and techniques used for planning, designing and developing computer programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software design lifecycle</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The tools, features and techniques used for planning, designing and developing computer programs

| Flowcharts | • What is a flowchart and what is its purpose?  
• Key terms and elements of a flowchart:  
  • sequences of actions  
  • inputs and outputs  
  • processes  
  • decisions  
  • direction of flow  
  • on/off page linkage.  
• When to use flowcharts.  
• Basic flowchart development procedure.  
• Advantages/disadvantages of flowcharts. |
|------------|------------------------------------------------------------------------------------|
| Pseudocode | • What is pseudocode and what is its purpose?  
• Key terms and elements of pseudocode.  
• How is pseudocode written?  
• Advantages/disadvantages of pseudocode. |
| Data tables | • What are data tables and what are their purposes?  
• Key features of data tables.  
• How are data tables used?  
• Advantages/disadvantages of data tables. |
### The tools, features and techniques used for planning, designing and developing computer programs

<table>
<thead>
<tr>
<th>Key features of computer programming languages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Variable or object types:</td>
<td></td>
</tr>
<tr>
<td>• single character</td>
<td></td>
</tr>
<tr>
<td>• integer</td>
<td></td>
</tr>
<tr>
<td>• real</td>
<td></td>
</tr>
<tr>
<td>• strings</td>
<td></td>
</tr>
<tr>
<td>• arrays</td>
<td></td>
</tr>
<tr>
<td>• pointers</td>
<td></td>
</tr>
<tr>
<td>• structures or records.</td>
<td></td>
</tr>
<tr>
<td>• Variables or objects scope:</td>
<td></td>
</tr>
<tr>
<td>• global</td>
<td></td>
</tr>
<tr>
<td>• local</td>
<td></td>
</tr>
<tr>
<td>• Declarations.</td>
<td></td>
</tr>
<tr>
<td>• Statements.</td>
<td></td>
</tr>
<tr>
<td>• Expressions.</td>
<td></td>
</tr>
<tr>
<td>• Assignments.</td>
<td></td>
</tr>
<tr>
<td>• Constructs:</td>
<td></td>
</tr>
<tr>
<td>• sequence</td>
<td></td>
</tr>
<tr>
<td>• selection:</td>
<td></td>
</tr>
<tr>
<td>• simple if</td>
<td></td>
</tr>
<tr>
<td>• nested if</td>
<td></td>
</tr>
<tr>
<td>• case type statement</td>
<td></td>
</tr>
<tr>
<td>• iteration:</td>
<td></td>
</tr>
<tr>
<td>• pre-condition loops</td>
<td></td>
</tr>
<tr>
<td>• post-condition loops</td>
<td></td>
</tr>
<tr>
<td>• Modularity and functions:</td>
<td></td>
</tr>
<tr>
<td>• arguments and parameters</td>
<td></td>
</tr>
<tr>
<td>• functions with no arguments and no return value</td>
<td></td>
</tr>
<tr>
<td>• functions with no arguments but do have a return value</td>
<td></td>
</tr>
<tr>
<td>• functions with arguments but no return value</td>
<td></td>
</tr>
<tr>
<td>• functions with arguments and a return value.</td>
<td></td>
</tr>
<tr>
<td>• Data structures:</td>
<td></td>
</tr>
<tr>
<td>• array</td>
<td></td>
</tr>
<tr>
<td>• First In, First Out (FIFO), eg Queue</td>
<td></td>
</tr>
<tr>
<td>• Last In, First Out (LIFO), eg Stack</td>
<td></td>
</tr>
<tr>
<td>• data files, eg text files, binary files (record) etc.</td>
<td></td>
</tr>
<tr>
<td>• Source files:</td>
<td></td>
</tr>
<tr>
<td>• valid program statements as defined by the language</td>
<td></td>
</tr>
<tr>
<td>• what are they used for?</td>
<td></td>
</tr>
<tr>
<td>The tools, features and techniques used for planning, designing and developing computer programs</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Algorithms</strong></td>
<td></td>
</tr>
<tr>
<td>• What are algorithms and what are their purposes?</td>
<td></td>
</tr>
<tr>
<td>• Classes of algorithm:</td>
<td></td>
</tr>
<tr>
<td>• simple recursive algorithms</td>
<td></td>
</tr>
<tr>
<td>• brute force algorithms</td>
<td></td>
</tr>
<tr>
<td>• randomised algorithms</td>
<td></td>
</tr>
<tr>
<td><strong>Testing – compiling and debugging computer programs</strong></td>
<td></td>
</tr>
<tr>
<td>• Testing techniques, eg:</td>
<td></td>
</tr>
<tr>
<td>• black box vs white box testing.</td>
<td></td>
</tr>
<tr>
<td>• Selecting test data, eg normal, extreme, invalid.</td>
<td></td>
</tr>
<tr>
<td>• Code coverage, eg percentage, logical pathways.</td>
<td></td>
</tr>
<tr>
<td>• Bench run and test run:</td>
<td></td>
</tr>
<tr>
<td>• actual vs. expected results</td>
<td></td>
</tr>
<tr>
<td>• screen captures etc</td>
<td></td>
</tr>
<tr>
<td>• remedial actions, eg code modification, bug fixes.</td>
<td></td>
</tr>
<tr>
<td>• Debug tools.</td>
<td></td>
</tr>
<tr>
<td>• Watches.</td>
<td></td>
</tr>
<tr>
<td>• Traces and step into.</td>
<td></td>
</tr>
<tr>
<td>• Breakpoints.</td>
<td></td>
</tr>
<tr>
<td>• Code inspection.</td>
<td></td>
</tr>
<tr>
<td>• Trace tables.</td>
<td></td>
</tr>
<tr>
<td>• Expected and actual results</td>
<td></td>
</tr>
<tr>
<td>• Releases and versioning, eg major/minor releases, patching, Concurrent Versioning System (CVS).</td>
<td></td>
</tr>
<tr>
<td>• Recording outcomes and recommendations, eg known bugs, common vulnerabilities and exposures (CVEs).</td>
<td></td>
</tr>
<tr>
<td><strong>Reviewing</strong></td>
<td></td>
</tr>
<tr>
<td>• Importance of regular project reviewing against specification requirements.</td>
<td></td>
</tr>
<tr>
<td>• Iterative project design and implementation process.</td>
<td></td>
</tr>
<tr>
<td><strong>Technical documentation</strong></td>
<td></td>
</tr>
<tr>
<td>• Clear, concise technical writing.</td>
<td></td>
</tr>
<tr>
<td>• Appropriate use of technical terminology.</td>
<td></td>
</tr>
<tr>
<td>• Suitable document structure and layout.</td>
<td></td>
</tr>
<tr>
<td>• Applicable for target audience.</td>
<td></td>
</tr>
<tr>
<td><strong>User documentation</strong></td>
<td></td>
</tr>
<tr>
<td>• Clear, concise ‘Plain English’ writing.</td>
<td></td>
</tr>
<tr>
<td>• Screen captures.</td>
<td></td>
</tr>
<tr>
<td>• Use cases.</td>
<td></td>
</tr>
<tr>
<td>• Lack of jargon.</td>
<td></td>
</tr>
<tr>
<td>• Use of only necessary technical terminology.</td>
<td></td>
</tr>
<tr>
<td>• Suitable document structure and layout.</td>
<td></td>
</tr>
<tr>
<td>• Applicable for target audience.</td>
<td></td>
</tr>
</tbody>
</table>
### Demonstrate the key features and functions of a client side scripting language

<table>
<thead>
<tr>
<th>Client-side languages</th>
<th>JavaScript elements and syntax</th>
<th>JavaScript syntax</th>
<th>Common language constructs</th>
<th>JavaScript functions</th>
<th>JavaScript objects</th>
<th>JavaScript events</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Types:</td>
<td>• Purposes (adding web page behaviour), eg:</td>
<td>• Identifiers, variables (local, global) and data types.</td>
<td>• Sequence.</td>
<td>• Declarations (name, parameters, code to be executed, return value).</td>
<td>• Objects (including primitive data types, eg Numbers, Booleans, Strings etc).</td>
<td>• Common HTML events, eg onblur, onchange, onclick, onmouseover, onmouseout, onkeydown, onload, onsubmit etc.</td>
</tr>
<tr>
<td>• scripting languages, eg JavaScript, VB Script, Adobe ActionScript</td>
<td>• change HTML element content via Document Object Model (DOM)</td>
<td></td>
<td>• Selection, eg if...else, nested if, switch.</td>
<td></td>
<td></td>
<td>• Adding events to HTML elements, eg Form elements (buttons, text box, etc).</td>
</tr>
<tr>
<td>• programming languages, eg Java.</td>
<td>• change HTML element attributes via DOM</td>
<td></td>
<td>• Iteration, eg pre-conditioned, post-conditioned, for...each mechanism.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Demonstrate the key features and functions of a client side scripting language

#### JavaScript debugging
- Debugging tools:
  - built-in web browser, eg Chrome developer tools, JavaScript console
  - third party, eg Firebug.
- Exception handling, try...throw...catch block.

### Demonstrate the key features and functions of a server side scripting language

#### Server-side languages
- Scripting frameworks and languages:
  - Java Server Pages (.jsp)
  - PHP
  - ASP classic.
- Operating system support.
- Commercial reputation.
- Market share and penetration.

#### Server-side script elements and syntax
- Purpose (creation of dynamic web page content, particularly when linked to a backend relational database system), validate HTML form input etc.
- Case sensitivity.

#### Identifiers
- Variables and constants (programming and system defined).
- Data Types, eg integer, decimal, Boolean, string, character, date/time, currency etc.
- Value range.
- Declaration and initialisation.
- Scope and visibility, eg public, private, local (module-level), global, namespaces etc.

#### Data structures
- Array, eg one-dimensional and multi-dimensional.
- Lists, Stacks, Queues.
- Text files, XML files.
- Relational databases (MySQL, MSSQL etc.), tables, records and fields.

#### Operators
- Arithmetic.
- Relational.
- Logical.
- Concatenation.

#### Common language constructs
- Sequence.
- Selection, eg if...else...endif, nested if, switch/case.
- Iteration, eg pre-conditioned, post-conditioned, for...each mechanism.
Demonstrate the key features and functions of a server side scripting language

**Functions**
- Programmer-defined functions:
  - naming and declaration
  - formal and actual parameters
  - function calls
  - return type.
- Common library functions:
  - input and output
  - arithmetic
  - string
  - date
  - file.
- Third party library functions.

**Server side classes and objects**
- Classes and objects (including primitive data types, eg Numbers, Booleans, Strings etc).
- Methods.
- Properties.

**HTTP request headers**
- Header content, eg posted values, URL encoded parameters.
- Accessibility of header content, eg.
- PHP Superglobals, eg $POST, $GET, $SESSION, $COOKIE etc.
- ASP .net Request object.
- limitations of header content, eg size, content.

**Accessing backend databases**
- Relational database management system (RDMS) overview.
- Proprietary software, eg MSSQL, Oracle etc.
- Open source (GPL), eg MySQL.
- Types of access:
  - command line
  - web-based interface, eg phpMyAdmin
  - database client, eg Oracle MySQL Workbench etc.
- Different database engines, their features and limitations.
- Username, password, hostname, TCP/IP Port.
- RDMS DDL (Data Definition Language) commands.
- RDMS DML (Data Manipulation Language) commands.
- RDMS DCL (Data Control Language) commands, eg GRANT, REVOKE of user permissions.
- Accessing backend database via web server scripting to:
  - select data (with where clause)
  - insert data
  - delete data
  - update data.
- Stored procedures, parameterised queries etc.
- Encryption and decryption, eg advanced encryption standard (AES).
Recognising vulnerabilities and countering threats to website and mobile technologies

| Common client-side threats | • Current trends and attack vectors.  
|                           | • Current and classic examples, eg:  
|                           |   • clickjacking  
|                           |   • HTML injection and cross-site scripting (XSS)  
|                           |   • Client-side cookies  
|                           |   • password autocomplete.  
|                           | • Current trends and attack vectors  
|                           | • Current and classic examples, eg:  
|                           |   • SQL injection  
|                           |   • directory traversal (“dot dot”, “..” notation, eg downloading unauthorised files)  
|                           |   • source code reveal (bad server configuration)  
|                           |   • remote file inclusion (untrusted sources)  
|                           |   • session hijacking, eg PHPSESSID  
|                           |   • non-patching of flawed code, eg ‘Heartbleed’.  
| Common server-side threats | • Current trends and attack vectors  
|                           | • Current and classic examples, eg:  
|                           |   • SQL injection  
|                           |   • directory traversal (“dot dot”, “..” notation, eg downloading unauthorised files)  
|                           |   • source code reveal (bad server configuration)  
|                           |   • remote file inclusion (untrusted sources)  
|                           |   • session hijacking, eg PHPSESSID  
|                           |   • non-patching of flawed code, eg ‘Heartbleed’.  
| Client side protection    | • Current and recommended techniques, eg:  
|                           |   • cache options (eg no cache, no autocomplete)  
|                           |   • client browser updates  
|                           |   • active cookie management (first vs. third party).  
| Server side protection    | • Current and recommended techniques, eg:  
|                           |   • server configuration and patching for web server, server side script engine and relational database  
|                           |   • secure sockets layer certification  
|                           |   • HTTP only cookies  
|                           |   • web vulnerability scanner, eg Acunetix  
|                           |   • awareness, eg common vulnerabilities and exposures (CVE) list  
|                           |   • use of non-standard ports for services, eg for relational database, web server, FTP, SSH access etc.  
| Mobile platforms and application | • Platforms types:  
| applications             |   • commercial deployment platforms, eg iOS (iPhone, iPad, iPod touch), Android, BlackBerry, Windows Phone, Symbian etc.  
|                           |   • free deployment platforms, eg Java ME, web browser etc.  
|                           | • Application types:  
|                           |   • native applications  
|                           |   • mobile web applications  
|                           |   • hybrid applications.  
| Reverse engineering      | • Forward engineering, ie typical translation process.  
|                           | • What is reverse engineering?  
|                           | • ‘Good’ and ‘bad’ reasons for reverse engineering.  
|                           | • Types of reverse engineering:  
|                           |   • static analysis  
|                           |   • dynamic analysis.  

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
## Recognising vulnerabilities and countering threats to website and mobile technologies

### Application hardening

- What is application hardening?
- Specific language issues, eg Java.
- Using improved coding techniques, eg:
  - code obfuscation
  - removal of debug code
  - improved exception handling
  - URL variable cleaning, eg missing parameters
  - protection from buffer overrun attacks
  - validation and stripping of HTML tags/JavaScript from inputs eg strip_tags() etc
  - update vulnerable code libraries
  - reduce storage of static information (eg passwords) in code.
- Using networking techniques, eg:
  - use SSL for data communication with servers etc
  - use of certificate pinning and pinsets in application.
- Using distribution techniques, eg:
  - MD5/SHA checksums for code distribution, preventing unauthorised modification.
- Using reviews, eg:
  - internal security review
  - external security review (eg Pentest).

## Key features and functions of operating system shell scripting

### Practical uses and scope

- Automated tasks, eg file maintenance, installation, batch jobs.
- Configuration management, eg disks, firewalls, network connections.

### Common languages

- Common examples, eg:
  - Sh, Bash (Linux) etc
  - PerlScript, Perl
  - MS Windows PowerShell
  - Windows Script Host (WSH)
  - MS Batch files
  - RubyScript, Ruby.
- Identification of shell script type by file extension.

### Command line interface (CLI)

- MS Windows CMD.exe, command.com.
- Linux Terminal.
- OS X Mac Terminal.
### Key features and functions of operating system shell scripting

**Access to operating system**

- Common commands, eg:
  - clearing screen
  - using user-defined variables
  - using environment variables
- files:
  - creating
  - deleting
  - renaming
  - moving
  - piping
- folders/directories:
  - change active
  - creating
  - deleting
  - renaming
  - moving
- processes:
  - start process
  - kill process
  - branching, eg if statements
  - loops, eg for, while, do etc
  - screen output
  - keyboard input
  - mapping network folders
  - functions
  - library objects, methods and properties, eg .Net framework.

**Debugging**

- Types of errors.
- Tools eg breakpoints, watch, trace etc.

### Key features and functions of data security and encryption

**Encryption and hashing**

- Principles of encryption:
  - symmetric-keys
  - public-key cryptography
  - hashing (one-way functions)
  - purpose of salting
  - key generation and size
  - blocks size.
- Common types of encryption:
  - ineffectual, eg ROT13, XOR
  - weak/withdrawn, eg data encryption standard (DES)
  - strong, eg advanced encryption standard (AES).
Performance outcomes

On successful completion of this unit, learners will be able to:

- **Performance outcome 1:** Demonstrate the tools, features and techniques used for planning, designing and developing computer programs.
- **Performance outcome 2:** Demonstrate the key features and functions of a client side scripting language.
- **Performance outcome 3:** Demonstrate the key features and functions of a server side scripting language.
- **Performance outcome 4:** Recognise vulnerabilities and counter threats to website and mobile technologies.
- **Performance outcome 5:** Demonstrate the key features and functions of operating system shell scripting.
- **Performance outcome 6:** Recognise the key features and functions of data security and encryption.

Grading criteria

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO1: Demonstrate the tools, features and techniques used for planning, designing and developing computer programs</strong></td>
<td><strong>The achieve a pass the learner must evidence that they can:</strong></td>
<td><strong>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</strong></td>
<td><strong>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</strong></td>
</tr>
<tr>
<td><strong>P1</strong></td>
<td>Outline the purpose and outcome of each of the stages of the software development lifecycle.</td>
<td><strong>M1</strong></td>
<td>Explain the advantages and disadvantages of any <strong>two</strong> SDLC models.</td>
</tr>
<tr>
<td><strong>P2</strong></td>
<td>Outline how flowcharts and pseudocode are used as methods of designing code and what elements make up a data table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P3</strong></td>
<td>Describe the key features of computer programming languages.</td>
<td><strong>M2</strong></td>
<td>Explain, with reference to <strong>two</strong> classes of algorithm, what they are and what their purpose is.</td>
</tr>
<tr>
<td>Performance outcomes</td>
<td>Pass</td>
<td>Merit</td>
<td>Distinction</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>PO2: Demonstrate the key features and functions of a client side scripting language</strong></td>
<td>The achieve a pass the learner must evidence that they can:</td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td>P4</td>
<td>Outline the contents and purpose of both user and technical documentation for a computer program.</td>
<td>M3</td>
<td>Explain the importance of testing with reference to two types of testing technique, and the tools used for carrying them out.</td>
</tr>
<tr>
<td>PO3: Demonstrate the key features and functions of a server side scripting language</td>
<td>P5</td>
<td>Use JavaScript elements to add interactive elements to a selected website.</td>
<td>M4</td>
</tr>
<tr>
<td>P6</td>
<td>Use debugging facilities to resolve errors in JavaScript elements.</td>
<td>M5</td>
<td>Apply a third-party JavaScript library function to perform a selected complex task.</td>
</tr>
<tr>
<td>P7</td>
<td>Create a JavaScript function to perform a selected complex task.</td>
<td>M6</td>
<td>Enhance a simple website by adding server-side validation and processing to its form-based content.</td>
</tr>
<tr>
<td>P8</td>
<td>Use server-side scripting elements to add dynamic content to a selected website.</td>
<td>M7</td>
<td>Create and use a bespoke server-side scripted class to solve a set task.</td>
</tr>
<tr>
<td>P9</td>
<td>Create and use a bespoke server-side scripted function to solve a set task.</td>
<td>M8</td>
<td></td>
</tr>
<tr>
<td>P10</td>
<td>Use server-side scripting to query data in a relational database system.</td>
<td>M9</td>
<td></td>
</tr>
<tr>
<td>P11</td>
<td>Use server-side scripting to manipulate data in a relational database system.</td>
<td>M10</td>
<td></td>
</tr>
<tr>
<td>Performance outcomes</td>
<td>Pass</td>
<td>Merit</td>
<td>Distinction</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PO4: Recognise vulnerabilities and counter threats to website and mobile technologies</td>
<td><strong>P12</strong> Identify four common client-side threats.</td>
<td><strong>M8</strong> Apply suitable measure to protect against a client-side threat in selected website solution.</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P13</strong> Identify four common server-side threats.</td>
<td><strong>M9</strong> Apply suitable measures to protect against a server-side threat in selected website solution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P14</strong> Outline three different mobile platforms and three different types of mobile application.</td>
<td><strong>M10</strong> Explain the two main types of reverse engineering and how it may be used for ‘good’ and ‘bad’ purposes.</td>
<td></td>
</tr>
<tr>
<td>PO5: Demonstrate the key features and functions of Operating System shell scripting</td>
<td><strong>P15</strong> Create a shell script to automate a set task, use a debugger to help identify any errors in the solution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO6: Recognise the key features and functions of data security and encryption</td>
<td><strong>P16</strong> Outline three different features of encryption.</td>
<td><strong>M11</strong> Compare and contrast two different types of encryption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Assessment amplification

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

There is no mandatory division of grading criteria although, as can be seen from the Grading criteria grid, some are naturally linked either by learning outcome or a developmental theme. Connections between the various pass, merit and distinction criteria can therefore suggest logical assessment grouping, but do not necessarily have to be followed.
Finding a single real world scenario to cover all the criteria is difficult. The key to assessment in this unit, as in others, is to make assessment a natural outcome of the learning experience, with skills being assessed at a level appropriate to the learner’s level of experience. The nature of the assessment technique is tutor-dependent, but some in this unit may only be achieved through generating working scripts to a good standard.

Assessments that connect this unit to others via connected tasks are also encouraged and it is possible that evidence produced during work for this unit may be used to provide evidence for criteria in other units.

For **P5** learners are required to create their own JavaScript functions to solve a complex task.

For **P15** the process that is to be automated should be a significant process involving several steps, not just deleting a file, for example.

For **M5** learners should identify, understand and use a suitable third-party library function to perform a complex task. The task may be the same as for **P5** and it must involve a multi-stage process, ie not be merely a simple one line calculation; many third-party libraries exist for JavaScript and there are none in particular that are mandated.

For **D4** learners should employ script or database functions to perform these encryptions and decryptions rather than command-line tools or utilities.

**Employer engagement guidance**

Where possible set problems encountered by the learner should have a strong vocational context; engaging with local SMEs (small and medium-sized enterprises) can provide a rich source of real world scenarios to investigate and solve.

A range of organisations exist that may help centres engage local employers in the delivery and potential assessment for this unit, for example The Tech-Partnership (thetechpartnership.com).

**Delivery guidance**

Although it is suggested that the content is delivered to follow the order of the learning outcomes in this unit specification, it is not the only sequence that could be used and tutors are encouraged to consider the holistic nature of the learner’s programme and the scheme itself. This is particularly evident for this unit where tutors may interleave various aspects (the development lifecycle, general programming features, client-side scripting and server-side scripting) to create more rounded and industry representative solutions.

Learners must have access to the hardware and software facilities necessary for the opportunity to generate evidence for all the grading criteria listed. If centres cannot guarantee these resources, the unit should not be attempted.

Delivery of tools and techniques is suggested to follow the pattern of a succession of small, but well chosen, exercises that form a developmental toolkit that learners may use to build more complex solutions. This type of approach gently builds confidence and self-sufficiency in the learners and is critical in promoting good problem-solving skills. Although remote web servers in shared environments may be used, it is beneficial for the learner to be able to observe server and client behaviour at close hand. Therefore it is preferable that a web server is installed on a local area network that the learners can access and inspect from the backend. This will permit access to some of the web server settings that can be obscured or unavailable in a shared hosting environment. Similar restrictions and levels of access should also apply to the relational database system that will be used by learners.
Performance outcome 1
Learners will begin their study of the unit by looking at how software is planned, designed and
developed in order to understand the stages of development and how security should be included from
the beginning. Learners will also need to be able to use some basic code design methods; pseudocode
and flowcharting should give them basic skills in this area.

Learners should be able to assess the utility of the various models and be able to compare two design
methods.

No particular programming language is mandated as a large variety is in current use. This particular
performance outcome will focus on the theoretical aspects of a language, but centres may choose to
use JavaScript and/or PHP as these will be used for later performance outcomes. Learners will review
the features of a programming language, what algorithms are and the processes of documenting,
testing and reviewing code.

Performance outcome 2
Focusing on client-side script through the use of JavaScript (although other client-side technologies
exist, its practical use is explicitly named here because of its ubiquity in the website development
process), learners will add interactive elements to a website and enhance a hypertext markup language
data form by adding client-side validation of its entries. They will develop skills in using debugging tools
to identify and resolve errors in their JavaScript code. The web pages requiring enhancement can be
supplied by the centre.

Using inbuilt functions and the creation of the learner's own JavaScript functions will help them to solve
a complex task. They are asked to consider suitable third-party library functions to perform a complex
task and should be able to identify them, judge their suitability and understand how they work.

Performance outcome 3
Performance outcome 3 switches the learner's focus to server-side scripting technologies. Here there
is no mandated server-side scripting language as the market share demonstrates multiple popular
development choices. Centres are advised to select and build a learner's skill in just one particular
server-side scripting language, although learners are required to be aware of competing alternatives
that may exist. Learners will create interactive website content via the chosen server-side scripting
language, possibly adding or refining functionality. Bespoke functions and classes should also become
familiar as they can contribute to solving a set task.

Learners will explore the connectivity and use of backend relational database systems, which are
particularly important in commercial websites.

Performance outcome 4
Learners will need to explore, recognise and counter threats to websites and mobile devices. Generally
these involve identifying and resolving client and server-side issues and reverse-engineering mobile
applications, while also considering the learner's ability to understand the level of threat involved and
evaluate which factors represent the most pressing danger.

Performance outcome 5
Learners will focus on creating a shell script to automate a repetitive task carried out by the operating
system. This should involve several steps and must not be just a single line command.
Performance outcome 6
Learners will be expected to have some knowledge of the relation of encryption to security, be able to compare different types of encryption and perform simple encryption and decryption of data.

Synoptic assessment guidance
Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

P3: Describe the key features of computer programming languages
Unit 1 – AO5: Demonstrate how computers process user requirements
Learners are introduced to the basic concept of a programming language and their different types and translation methods through this assessment outcome. This is likely to provide a sound foundation for the learner to tackle this grading criterion.

P5: Use JavaScript elements to add interactive elements to a selected website
P7: Create a JavaScript function to perform a selected complex task
Unit 1 – AO5: Demonstrate how computers process user requirements
This unit introduces the key features of high level languages such as JavaScript and examples provided for this client-side scripting language could support the learner when adding interactive elements to a selected website, depending on the depth of coverage chosen.

Unit 5 – PO2: Understanding and applying computer logic
Most functions that perform complex tasks will typically involve the application of Boolean logic in order to process the data successfully. Learners may rely on the introduction to this concept that is provided through the second performance outcome of this unit.

P10: Use server-side scripting to query data in a relational database system
P11: Use server-side scripting to manipulate data in a relational database system
Unit 1 – AO3: Evaluate the software requirements of a computer system
This unit’s third assessment outcome introduces the concept of application software and would, typically, include the role of the relational database system in modern computer. As a direct consequence, learners should understand the concept of a relational database system, how it is structured, queried and manipulated.

Unit 1 – AO5: Demonstrate how computers process user requirements
This unit introduces the key features of fourth generation languages (4GL) such as Structured Query Language (SQL). Server-side scripting languages typically use a combination of library functions and SQL syntax to successfully query data in a relational database system. Examples provided for this particular 4GL could support the learner when generating the appropriate server-side scripting code needed for this performance outcome, depending on the depth of coverage chosen.
P12: Identify four common client-side threats

Unit 1 – AO3: Evaluate the software requirements of a computer system
Many of the common client-side threats (e.g., tracking cookies) can be detected by the type of security software that is introduced in this unit’s assessment outcome. Antivirus and anti-spyware software are particularly prevalent in the identification of common client-side threats and may provide the learner with additional information about the nature and spread of the risk.

P13: Identify four common server-side threats

Unit 4 – PO2: Analyse security issues for a network
Many server-side threats are associated with the services that are running, not just the exploitation of common code vulnerabilities. This unit’s second performance outcome introduces many of the threats that target web servers and database servers. Learners should appreciate the symmetry here; in this unit they are being taught good coding practice and how to protect against these threats to web and database servers (and services).

P16: Outline three different features of encryption

Unit 1 – AO3: Understand the software requirements of a computer system
Encryption is introduced as a type of security software in this unit, providing the learner with a sound foundation before they encounter it in practical situation.

Unit 3 – PO2: Identify the different types of network architectures and technology types
Different encryption methods are a key technique for securing wireless networks. Concepts introduced here should be familiar to learners through using their own wireless devices and form a good reference point for understanding encrypted and unencrypted data and the use of different types of keys.

Unit 6 – AO2: Explain the controls that an organisation needs to implement to manage risks
This unit’s second assessment outcome explores the concept of acceptable encryption as part of the suite of network security policies that form the controls that manage risks in an organisation. From a learner’s perspective, this is helpful as the feature set of an encryption method often determines whether they are fit for purpose.

Unit 6 – AO5: Explain operational security management and analyse how incidents are managed
Cryptography forms a key security concern when considering how incidents are managed. This includes different suites, the management of keys and digital signatures.

Unit 6 – AO7: Explain the scope, procedures and reporting processes of a penetration test
This unit’s seventh assessment outcome focuses on the process and content of a typical penetration test. Encryption is a key aspect of any penetration test, including checks on weak or badly applied cipher suite and how encryption may be used by a web application (including its backend database) and its transmission methods, e.g., SSL. The learner should find that a firm understanding of the features of different cipher suites should assist the confident writing and practical interpretation of a penetration test.

Unit 7 – PO1: Select hardware and software to promote security for a network system
This unit’s focus is on data and its accessibility, including a detailed examination of the use of cryptographic algorithms and protocols. Consequently it introduces many of the types, strengths, weaknesses and mechanisms of many different cipher suites. Learners should benefit from the underpinning knowledge presented here in tackling this criterion.

Unit 9 – PO2: Plan a computer forensic investigation
Learners should find that using specialist software tools to decrypt suspect data files complements their understanding of the different types of encryption available (and their respective features).
Useful links and resources

Books

Websites
- Code Academy: codeacademy.com
- CODE: code.org/learn
- CVE – Common Vulnerabilities and Exposures: cve.mitre.org
- How-to Geek: howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics
- jQuery:jquery.com
- JSFiddle: jsfiddle.net
- Linux shell scripting: freeos.com/guides/isst
- MySQL: mysql.com
- OWASP – Open Web Application Security Project: owasp.org
- PHP: php.net
- Sitepoint: reference.sitepoint.com
- W3Schools – Online Web Tutorials: W3schools.com
- Webplatform.org: webplatform.org
- WIKIBOOKS: en.wikibooks.org/wiki/Windows_Batch_Scripting
- wiseGEEK: wisegeek.org/what-is-an-algorithm.htm
### 12.9 Unit 9: Computer forensic investigation (optional)

<table>
<thead>
<tr>
<th>Title</th>
<th>Computer forensic investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit number</td>
<td>R/507/6440</td>
</tr>
<tr>
<td>Unit assessment type</td>
<td>Centre assessed and externally quality assured</td>
</tr>
<tr>
<td>Recommended assessment method</td>
<td>Practical assignment</td>
</tr>
<tr>
<td></td>
<td>This is the preferred assessment method for this unit. A centre may choose an alternative method of assessment, but will be asked to justify as part of the quality assurance process.</td>
</tr>
<tr>
<td>Guided learning hours</td>
<td>90</td>
</tr>
<tr>
<td>Transferable skill(s)</td>
<td>Communication (oral)</td>
</tr>
</tbody>
</table>

#### Resources required for this unit
A range of physical computing resources such as:
- workstations
- personal computers
- modems or other connectivity devices
- printers
- hard drives
- DSL modems
- monitors
- switches
- hubs
- other peripheral devices
- forensic software tools
- forensic hardware tools
- PDAs, mobile phones, tablets etc.

#### Synoptic assessment within this unit
IT: Cyber Security and Security Administration linked to Units 1 and 4.

Draws on experience and knowledge of different types of software, particularly systems software (operating systems and utilities) as discussed in Unit 1.

Many of the risks associated with the hardware and software in a computer system can potentially affect the security of an organisation and, as such, are often identified as threats in Unit 4.

A signposted breakdown can be found in this unit’s synoptic assessment guidance.

### Aim and purpose
To equip learners with the necessary knowledge and practical ability to carry out a range of forensic analysis on computer systems by acquiring and preserving the integrity of the evidence, investigating and analysing results and presenting the results of their investigations and analysis.

---

7 Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.
Unit introduction

Computer forensics is the use of analytical and investigative techniques that would enable someone to identify, gather and examine digitally stored or encoded information thereby providing digital evidence of specific or general activity. It is used in the detection and prevention of crime or any other dispute where the evidence is digitally stored.

As businesses become more complex and exchange more and more information online, these crimes are on the increase. The computer forensic industry has become a science in itself and the number of organisations and professionals offering computer forensic services has increased dramatically over the last few years.

This unit provides an opportunity to evidence achievement of the transferable skill of communication (oral).

Forensic computer analysts investigate cybercrime and should have an excellent working knowledge of all aspects of computer systems to include hardware, software, storage media, networking and encryption. Forensic computer analysts must have good communication skills, as they will be required to present the results of their investigations to a wide audience comprising technical and non-technical specialists.

Learners will enhance their understanding of the importance of careful planning in order to ensure that the integrity of the equipment and data is preserved as well as the use of a wide variety of software and hardware tools that can support investigations. They will gain an understanding of the importance of careful documentation of activities carried out and the consequences if due process is not followed.
## Unit content

### The principles of computer forensic investigation

#### Hardware risks and unauthorised usage

- Portability.
- Theft potential.
- Potential breach of physical security:
  - searching rubbish bins (searching through materials that have been thrown away).
- Deleted files not erased from the system.
- Breaches of communication security:
  - wiretapping
  - emanation eavesdropping.
- Denial or degradation of service.
- Potential breach of personal security:
  - masquerading (using the identity of another to access a system)
  - piggybacking (following an authorised person into a location).
- Risks associated with mobile devices:
  - cloning
  - re-programming (unblocking)
  - deliberate interference
  - jamming
  - fraud and financial criminal acts
  - harassment.
- Risks associated with other hardware devices eg illegal theft of data by using:
  - CDs/DVDs
  - CD/DVD ROM/RW drives
  - Blu-ray disks and drives
  - zip drives and disks
  - USB flash drives
  - external hard drives
  - older technology eg tape drives and floppy disks.

#### Unauthorised hardware

- Modems.
- Key loggers.
- I/O devices.
- USB devices.
- FireWire devices.
- Bluetooth devices.
- eSATA.
- Wireless devices.
<table>
<thead>
<tr>
<th><strong>The principles of computer forensic investigation</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risks associated with software</strong></td>
<td><strong>Breaches of communications and data security:</strong></td>
</tr>
<tr>
<td></td>
<td>• IP spoofing</td>
</tr>
<tr>
<td></td>
<td>• password sniffing</td>
</tr>
<tr>
<td></td>
<td>• scanning</td>
</tr>
<tr>
<td></td>
<td>• excess privileges</td>
</tr>
<tr>
<td></td>
<td>• data attacks, eg:</td>
</tr>
<tr>
<td></td>
<td>• unauthorised copying of data</td>
</tr>
<tr>
<td></td>
<td>• traffic analysis</td>
</tr>
<tr>
<td></td>
<td>• covert channels</td>
</tr>
<tr>
<td></td>
<td>• data diddling</td>
</tr>
<tr>
<td></td>
<td>• software attacks, eg:</td>
</tr>
<tr>
<td></td>
<td>• trap door/back door</td>
</tr>
<tr>
<td></td>
<td>• session hijacking</td>
</tr>
<tr>
<td></td>
<td>• tunnelling</td>
</tr>
<tr>
<td></td>
<td>• timing attacks</td>
</tr>
<tr>
<td></td>
<td>• trojan horses</td>
</tr>
<tr>
<td></td>
<td>• viruses and worms</td>
</tr>
<tr>
<td></td>
<td>• salamis</td>
</tr>
<tr>
<td></td>
<td>• logic bombs.</td>
</tr>
<tr>
<td><strong>Understand file systems and data storage</strong></td>
<td><strong>FAT, eg:</strong></td>
</tr>
<tr>
<td></td>
<td>• FAT 16</td>
</tr>
<tr>
<td></td>
<td>• FAT 32 (Virtual FAT or VFAT)</td>
</tr>
<tr>
<td></td>
<td>• Extended FAT (exFAT).</td>
</tr>
<tr>
<td></td>
<td>• NTFS.</td>
</tr>
<tr>
<td></td>
<td>• File system metadata.</td>
</tr>
<tr>
<td></td>
<td>• Live, deleted, unallocated data and file stack.</td>
</tr>
<tr>
<td><strong>Preinstalled OS tools (eg)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event viewer.</td>
</tr>
<tr>
<td></td>
<td>• Firewall.</td>
</tr>
<tr>
<td><strong>Planning a computer forensic investigation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Evidence life cycle</strong></td>
<td><strong>Collection and identification.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Storage, preservation and transportation.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Presentation of evidence.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Return to owner or court.</strong></td>
</tr>
</tbody>
</table>
## Planning a computer forensic investigation

### Four steps of computer forensic investigation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquisition:</strong></td>
<td></td>
</tr>
<tr>
<td>• search and seizure:</td>
<td></td>
</tr>
<tr>
<td>• voluntary surrender</td>
<td></td>
</tr>
<tr>
<td>• subpoena</td>
<td></td>
</tr>
<tr>
<td>• search warrant.</td>
<td></td>
</tr>
<tr>
<td><strong>Identification:</strong></td>
<td></td>
</tr>
<tr>
<td>• relevance of evidence:</td>
<td></td>
</tr>
<tr>
<td>• proves or disproves facts in a case</td>
<td></td>
</tr>
<tr>
<td>• admissibility of evidence</td>
<td></td>
</tr>
<tr>
<td>• legal collection of evidence</td>
<td></td>
</tr>
<tr>
<td>• not modifying evidence after it has been seized</td>
<td></td>
</tr>
<tr>
<td>• protect the chain of custody</td>
<td></td>
</tr>
<tr>
<td>• treat each incident as a criminal act</td>
<td></td>
</tr>
<tr>
<td>• leave no trace, eg ensuring media is not modified or includes trace that it has been accessed</td>
<td></td>
</tr>
<tr>
<td>• read-only images</td>
<td></td>
</tr>
<tr>
<td>• software write blocker</td>
<td></td>
</tr>
<tr>
<td>• hardware write blocker</td>
<td></td>
</tr>
<tr>
<td>• types of evidence:</td>
<td></td>
</tr>
<tr>
<td>• real evidence, eg actual physical evidence</td>
<td></td>
</tr>
<tr>
<td>• documentary evidence, eg log files, database files, incident-specific files, reports (best evidence rule – original documents not copies)</td>
<td></td>
</tr>
<tr>
<td>• testimonial evidence, eg witness testimony</td>
<td></td>
</tr>
<tr>
<td>• demonstrative evidence, eg use of visual aids and other illustrations.</td>
<td></td>
</tr>
<tr>
<td><strong>Computer forensic software tools:</strong></td>
<td></td>
</tr>
<tr>
<td>• disk tools and capture</td>
<td></td>
</tr>
<tr>
<td>• disk imaging software</td>
<td></td>
</tr>
<tr>
<td>• software or hardware write tools</td>
<td></td>
</tr>
<tr>
<td>• hashing tools</td>
<td></td>
</tr>
<tr>
<td>• file recovery programs</td>
<td></td>
</tr>
<tr>
<td>• analysis software, eg to search and evaluate Internet cookies</td>
<td></td>
</tr>
<tr>
<td>• encryption decoding software</td>
<td></td>
</tr>
<tr>
<td>• password cracking software</td>
<td></td>
</tr>
<tr>
<td>• acquisition of website software</td>
<td></td>
</tr>
<tr>
<td>• network analysis tools</td>
<td></td>
</tr>
<tr>
<td>• network discover and security auditing</td>
<td></td>
</tr>
<tr>
<td>• extraction of RAM dumps</td>
<td></td>
</tr>
<tr>
<td>• mounting forensic logical and physical disks as read-only.</td>
<td></td>
</tr>
<tr>
<td><strong>Email analysis.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>File signatures.</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Planning a computer forensic investigation

<table>
<thead>
<tr>
<th>Four steps of computer forensic investigation continued</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mac OS tools eg Mac Memory Reader.</td>
<td></td>
</tr>
<tr>
<td>• Mobile devices eg phone analyser.</td>
<td></td>
</tr>
<tr>
<td>• Data analysis.</td>
<td></td>
</tr>
<tr>
<td>• File viewers.</td>
<td></td>
</tr>
<tr>
<td>• Internet analysis.</td>
<td></td>
</tr>
<tr>
<td>• Registry analysis.</td>
<td></td>
</tr>
<tr>
<td>• Application analysis.</td>
<td></td>
</tr>
<tr>
<td>• Presentation of evidence:</td>
<td></td>
</tr>
<tr>
<td>• audience</td>
<td></td>
</tr>
<tr>
<td>• chain of custody:</td>
<td></td>
</tr>
<tr>
<td>• date</td>
<td></td>
</tr>
<tr>
<td>• step-by-step process of each activity</td>
<td></td>
</tr>
<tr>
<td>• explanation of activity, ie what it involves</td>
<td></td>
</tr>
<tr>
<td>• controls to maintain integrity of evidence eg taking photographs</td>
<td></td>
</tr>
<tr>
<td>• list of procedures used during collection process with justification of actions</td>
<td></td>
</tr>
<tr>
<td>• precautions taken to preserve state of evidence eg precautions against disk drive damage</td>
<td></td>
</tr>
<tr>
<td>• controls to prevent accidental changes to the evidence, eg implementing a write blocker.</td>
<td></td>
</tr>
</tbody>
</table>
Computer forensic investigation

Documenting the investigation

- Purpose of the documentation, eg to support chain of custody:
  - date and time of action
  - action type (choose one dependent on activity being undertaken):
    - initial evidence collection
    - evidence location change
    - removal of evidence for analysis
    - return evidence to storage
  - personnel collecting/accessing evidence
- computer descriptive information:
  - computer make and model
  - serial number(s)
  - location
  - additional ID information
  - BIOS settings specific to disk drives
- disk drive descriptive information:
  - disk drive manufacturer, model number and serial number
  - drive parameters (eg heads, cylinders, sectors per track)
  - jumper setting
  - computer connection information (eg adapter, master/slave)
- handling procedure:
  - preparation (eg static grounding, prevention of physical shock etc)
  - contamination precautions taken
  - step-by-step procedure taken during each event
  - inventory of supporting items created/acquired eg hask or checksum of drive/files
- complete description of action:
  - procedure followed
  - tools used
  - step-by-step description of analysis and results
- reason for action taken
- notes:
  - comments not requested anywhere within log
  - additional details that arise as the investigation is carried out.
- Collection of evidence.
- Analysis of evidence.
- Review of evidence.
- Documentation of evidence.
Presenting computer forensic evidence

| Present computer forensic evidence | • Audience.  
| | • Purpose.  
| | • Documentary, eg reports, logs etc.  
| | • Physical evidence, eg photographs, items of equipment.  
| | • Simulation, eg simulating activities to present an argument.  
| | • Presenting the facts:  
| | • what you did  
| | • why you did it  
| | • how you did it  
| | • what you found.  

Performance outcomes

On successful completion of this unit learners will be able to:

- **Performance outcome 1:** Understand the principles of computer forensic investigation.
- **Performance outcome 2:** Plan a computer forensic investigation.
- **Performance outcome 3:** Carry out a computer forensic investigation.
- **Performance outcome 4:** Present computer forensic evidence.

Grading criteria

<table>
<thead>
<tr>
<th>Performance outcomes</th>
<th>Pass</th>
<th>Merit</th>
<th>Distinction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To achieve a pass the learner must evidence that they can:</strong></td>
<td>In addition to the pass criteria, to achieve a merit the evidence must show the learner can:</td>
<td>In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:</td>
<td></td>
</tr>
<tr>
<td><strong>PO1: Understand the principles of computer forensic investigation</strong></td>
<td><strong>P1</strong> Outline eight potential risks associated with the hardware of a computer system.</td>
<td><strong>M1</strong> Explain the issues associated with four examples of unauthorised hardware.</td>
<td></td>
</tr>
<tr>
<td><strong>P2</strong> Outline eight potential risks associated with the software of a computer system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P3</strong> Describe the file systems of a computer system.</td>
<td><strong>M2</strong> Explain the data storage on a computer system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance outcomes</td>
<td>Pass</td>
<td>Merit</td>
<td>Distinction</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>PO2: Plan a computer forensic investigation</strong></td>
<td><strong>P4</strong> Explain how two pre-installed OS tools can contribute to forensic information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P5</strong> Create an annotated diagram of the evidence lifecycle.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P6</strong> Explain the admissibility of evidence providing four examples of good practice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P7</strong> Identify the types of evidence that could be gathered from the forensic investigation.</td>
<td><strong>M3</strong> Justify the types of evidence selected.</td>
<td><strong>D1</strong> Explain the precautions that will be taken to preserve the state of each type of evidence selected.</td>
</tr>
<tr>
<td></td>
<td><strong>P8</strong> Select the following tools to analyse the evidence:  - software tools  - hardware tools.</td>
<td><strong>M4</strong> Justify the computer forensic tools selected.</td>
<td><strong>D2</strong> Explain the importance of the chain of custody process.</td>
</tr>
<tr>
<td><strong>PO3: Carry out a computer forensic investigation</strong></td>
<td><strong>P9</strong> Carry out the forensic investigation on the selected system using forensic tools to investigate data and hardware, taking the necessary steps to document and preserve the integrity of the evidence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>P10</strong> Record the results of the forensic investigation.</td>
<td><strong>M5</strong> Interpret the results of the forensic investigation.</td>
<td><strong>D3</strong> Complete Chain of Custody documentation.</td>
</tr>
<tr>
<td><strong>PO4: Present computer forensic evidence</strong></td>
<td><strong>P11</strong> Present the outcome of the computer forensic investigation.</td>
<td><strong>M5</strong> Interpret the results of the forensic investigation.</td>
<td></td>
</tr>
</tbody>
</table>
### Performance outcomes

**Pass**

To achieve a pass the learner must evidence that they can:

- P12 Provide physical evidence from the computer forensic investigation.

**Merit**

In addition to the pass criteria, to achieve a merit the evidence must show the learner can:

- M6 Review the computer forensic investigation process.

**Distinction**

In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:

- In addition to fulfilling the pass and merit criteria, to achieve a distinction the evidence must show that the learner can:

### Assessment amplification

This section provides amplification of what is specifically required or exemplification of the responses learners are expected to provide.

In completing P11, learners will be presented with an opportunity to demonstrate the transferable skill of communication (oral).

**Note:** Learners could be provided with a computer system linked to a detailed scenario, which would enable them to provide evidence holistically across the unit.

Learners must be given access to a computer system that they will be able to use to plan their forensic investigation. To enable learners to present evidence holistically, it is recommended that the scenario that they are given requires them to present physical evidence as well as documentary evidence.

For P7 learners are required to identify the different types of evidence that could be collected, which could include real, documentary, testimonial and/or demonstrative evidence depending on the investigation to be undertaken.

For M3 learners are required to justify why they have selected the types of evidence identified in P7 explaining why it is relevant to the investigation and what it could provide or disprove.

For P10 the learners must preserve the integrity of the evidence that they have selected as being appropriate to the investigation. The evidence could include photographs, videos and/or a detailed witness testimony from the teacher. The witness testimony must clearly explain what the learner did in order to preserve integrity.

For D3 learners must complete the Chain of Custody documentation ensuring that the bullet points within the unit content for PO3 have been addressed. The evidence will be the Chain of Custody document.

For P13 learners are required to present the outcome from the investigation to an intended audience, eg the management team of an organisation, a courtroom etc. How they present their findings can be affected by the audience. The evidence could be presented as a video of the learner presenting to their audience supported by their documentary evidence, a presentation with speaker notes supporting their documentation or a report supported by documentary evidence. This documentary evidence would include any reports, logs, testimonies and if appropriate Chain of Custody document. The learners’ presentations must include what they did, why they did it, how they did it and what they found.
To achieve **P14** learners must present the physical evidence to support P13. This may be photographs or equipment. It may require the learners to set up a physical simulation in order to aid the presentation of their findings. This can be evidenced via photographs, video and/or witness testimonies. Any photographic evidence used as part of their evidence would also provide evidence for this assessment criterion.

To achieve **M7** learners must review the process they followed to carry out the computer forensic investigation. The review must include the methods used, the outcomes of the investigation as well as drawing conclusions as to whether it was effective or not. They should consider whether there was anything they would do better if presented with a similar scenario. Did they have any problems and how did they overcome them?

**Employer engagement guidance**

If learners are in the workplace then the centre could ask the employer whether there were any suitable projects that the learners could work on as part of the team. It would be helpful for the employer to be made aware of the sort of skills that the learners have to practice.

**Delivery guidance**

**Performance outcome 1**

Learners could be divided into small groups and provided with different computer systems where they could identify the different hardware, software, file systems and data storage they contain. Additional hardware could be added to the systems that they are investigating to prompt them into considering whether these additions are unauthorised.

It is important that learners have the opportunity to look at a variety of different computer systems (ie standalone, networked etc) using different operating systems so that they have access to, not only Windows operating systems, but UNIX and Linux. They could be asked to research whether the different operating systems have pre-installed auditing tools that could be used to support computer forensic investigations.

**Performance outcome 2**

Through class discussions and/or through individual research, learners should consider what makes evidence inadmissible when carrying out an investigation. This could lead to them researching how the integrity of the evidence could be preserved.

Learners need to consider different types of evidence and identify which category they fall under as well as identifying evidence that meets the ‘best evidence rule’.

Small groups of learners could be tasked with researching different computer forensic software and hardware tools that are available and presenting the results of their research to the rest of the group. They need to be able to explain the purpose of the tool as well as how and why it is used.

Learners should be made aware of the ‘Chain of Custody’ requirements as well as how and why it is important that activities are documented carefully.

Small groups of learners could be given a variety of computer systems, that have evidence of cybercrime for which they have to plan how they will carry out their investigations. The planning should include:

- what evidence they will be collecting and why
- how they will preserve the integrity of the evidence
- what software and/or hardware forensic tools they will use
- what documentary evidence they will need to collect and/or complete.
Performance outcome 3

Learners need to be given the opportunity to practice carrying out a forensic investigation of a variety of different computer systems, eg standalone, network, Windows, Linux, UNIX. These activities could be a follow on from the activities that took place to enable them to plan their investigations. It is important that learners follow their plans and maintain the integrity of the evidence. They should document the activities carefully in the ‘Chain of Custody’ documentation as well as gather any additional evidence that comes to light during the investigation, ie not just the anticipated evidence identified as part of their planning.

Performance outcome 4

Learners should be encouraged to consider how they would present the results of their computer forensic investigation to a variety of different audiences, eg the management team of an organisation, a courtroom, a technical and non-technical audience.

The presentations could include role-play where the learners are asked questions based on the evidence that they have presented, which would require them to justify some of the actions taken and the validity of the evidence. It is important that learners understand the importance of the evidence that they present and that this includes detailed documentation within the ‘Chain of Custody’ document as well as other supporting documentation, eg event log etc.

Learners could be provided with a scenario that would encourage them to simulate the incident to aid their explanations to their audience.

Synoptic assessment guidance

Synoptic assessment is a mandatory requirement of all AQA Tech-levels and this qualification has been designed with synoptic learning and assessment at its heart. Units link to each other providing development on concepts and topics, reinforcing learning and skill development which enables learners to bring knowledge and skills from other units to contribute to the assessment of units as shown. Being able to work synoptically is the cornerstone of work-based problem-solving as learners make judgements on assessed prior learning in the context of new situations.

The mapping provided below shows where opportunities to undertake synoptic assessment can be found across the units of this qualification. Centres must ensure that these opportunities are built into their programmes of learning and assessment activities.

**P1: Outline eight potential risks associated with the hardware of a computer system**

Unit 4 – PO2: Analyse security issues for a network
Many of the potential risks the learner needs to describe here are often viewed as internal and external threats, being discussed in other units. Learners should be able to link some of the threats that organisations commonly face to hardware issues.

**P2: Outline eight potential risks associated with the software of a computer system**

Unit 4 – PO2: Analyse security issues for a network
Many of the potential risks the learner needs to describe here are often viewed as internal and external threats, being discussed in other units. Learners should be able to link some of the threats that organisations commonly face to software issues.

Unit 1 – AO3: Understand the software requirements of a computer system
Many of the risks sought here are tackled by the common software-based security measures (eg VPN, encryption, firewalls, antivirus, etc) discussed in this unit. Learners should benefit from the practical time they have with these software tools and use the experience to enhance their descriptions.
### P3: Describe the file systems of a computer system

**Unit 1 – AO3: Understand the software requirements of a computer system**

Learners are introduced to seven different types of file system in Unit 1 and should be able to reference this material to enhance their descriptions for this grading criterion.

### P4: Explain how two preinstalled OS tools can contribute to forensic information

**Unit 1 – AO3: Understand the software requirements of a computer system**

One of the preinstalled OS tools required here (firewall) is introduced to the learner in this unit. Learners should benefit from the practical time they have with this software tool to use the experience to enrich their coverage.

### P8: Select the following tools to analyse the evidence:

- software tools
- hardware tools.

**Unit 1 – AO3: Understand the software requirements of a computer system**

Many units furnish the learner with opportunities to use the tools they are likely to select to analyse the evidence from a computer forensic investigation. Experience of using these tools in other situations will help the learner evaluate their functionality and applicability to the task at hand.

### Useful links and resources

**Books**


**Websites**

- [scoop.it/t/computer-forensics-will-get-you](http://scoop.it/t/computer-forensics-will-get-you)
13 Externally set and marked examinations

13.1 Introduction

The Foundation Technical Level (360 GLH) in IT: Cyber Security (TVQ01010) qualification units Y/507/6424 (Fundamental principles of computing) and H/507/6426 (Communication technologies) are assessed via an externally set and marked AQA examination.

The Technical Level (720 GLH) in IT: Cyber Security and Security Administration (TVQ01009) qualification unit J/507/6435 (Network and cyber security administration) is assessed via an externally set and marked AQA examination.

External examinations are set by AQA (sometimes in collaboration with an employer or a professional body) and are sat by learners in a controlled examination environment, at a preset time and date and marked by AQA.

Examinations are available for externally assessed units in January and June and entries must be made in accordance with AQA's procedures.

Further information on how to make entries for examinations can be found in the AQA Centre Administration Guide for Technical and Vocational Qualifications.
13.2 Examination format and structure

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Fundamental principles of computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam sessions</td>
<td>January and June</td>
</tr>
<tr>
<td>Duration</td>
<td>2 hours</td>
</tr>
<tr>
<td>Type of exam</td>
<td>Written exam</td>
</tr>
<tr>
<td></td>
<td>A mixture of multiple choice, short answer and case study type questions.</td>
</tr>
<tr>
<td>Number of marks</td>
<td>80</td>
</tr>
<tr>
<td>Weighting of unit</td>
<td>25% of IT: Cyber Security (TVQ01010)</td>
</tr>
<tr>
<td></td>
<td>12.5% of IT: Cyber Security and Security Administration (TVQ01009)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Communication technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam sessions</td>
<td>January and June</td>
</tr>
<tr>
<td>Duration</td>
<td>2 hours</td>
</tr>
<tr>
<td>Type of exam</td>
<td>Written exam</td>
</tr>
<tr>
<td></td>
<td>A mixture of multiple choice, short answer and case study type questions.</td>
</tr>
<tr>
<td>Number of marks</td>
<td>80</td>
</tr>
<tr>
<td>Weighting of unit</td>
<td>25% of IT: Cyber Security (TVQ01010)</td>
</tr>
<tr>
<td></td>
<td>12.5% of IT: Cyber Security and Security Administration (TVQ01009)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Network and cyber security administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam sessions</td>
<td>January and June</td>
</tr>
<tr>
<td>Duration</td>
<td>2 hours</td>
</tr>
<tr>
<td>Type of exam</td>
<td>Written exam</td>
</tr>
<tr>
<td></td>
<td>A mixture of multiple choice, short answer and case study type questions.</td>
</tr>
<tr>
<td>Number of marks</td>
<td>80</td>
</tr>
<tr>
<td>Weighting of unit</td>
<td>12.5% of IT: Cyber Security and Security Administration (TVQ01009)</td>
</tr>
</tbody>
</table>

13.3 Reasonable adjustments and special considerations

Information on the reasonable adjustments allowed for the external examinations within this qualification can be found in the AQA Centre Administration Guide for Technical and Vocational Qualifications.

13.4 Availability of past examination papers

Sample and past examination papers for this qualification are available from AQA.
14 External quality assurance

14.1 Overview

AQA’s approach to quality assurance for this qualification is described within each unit specification.

External quality assurance for Tech-levels takes the form of verification and is concerned with maintaining the quality of assessment and checking that the assessment process has been undertaken appropriately by centre staff. It focuses on auditing the whole process and enables the head of centre, and all individuals involved in the assessment process, to understand what is required by them.

14.2 Quality assurance visits

When a learner is registered or a centre wants to submit work, this triggers a verification visit from an AQA external quality assurer (EQA).

Once a centre has registered learners, these visits will occur, as a minimum, every six months and will be face-to-face at a centre.

Our EQAs offer advice and guidance on any aspect of quality assurance in between formal visits, via telephone or email, and additional visits can be arranged.

These meetings will involve verifying that:

- all of the staff, resources, processes and procedures are still in place
- the centre is continuing to meet the approved centre criteria (those signed off during the initial centre approval visit)
- there is evidence of meaningful employer involvement in delivery.

A major part of the verification process is to check that the centre’s policies and procedures (including internal standardisation minutes, record keeping, IQA/assessor records and materials) meet AQA’s requirements and ensure valid and reliable assessment.

The EQA will look at a representative sample of learner work to verify that the results awarded by the centre are valid, as well as reviewing evidence of the activities that have been undertaken to standardise assessments.

These samples will be taken from different sites if the centre operates at more than one location, from different centre assessors or IQAs and at different stages of delivery – all samples will be selected by the EQA.

As part of the sample, the EQA will request examples of learner work at Pass, Merit and Distinction. This will also support the centre in their internal standardisation.

If centre assessment decisions are found to be inconsistent, adjustments can be made (at a learner and cohort level) or in more severe cases (where a fundamental inconsistency or non-compliance is identified), sanctions (from a Level 1: Action plan through to Level 4: Suspension of delivery) can be put in place.
14.3 Sanctions

Sanctions are used to help process improvement and are a way of protecting the validity of assessments or assessment decisions. We will only ever impose sanctions on a centre that are proportionate to the extent of the risk identified during the quality assurance process.

Sanctions can be applied at a learner, centre or centre staff level – and they can be at qualification or centre level and take the following form:

Level 1: Action point in EQA report
Level 2: Suspension of direct claims status (where applicable)
Level 3: Suspension of learner registration and/or certification
Level 4: Withdrawal of centre approval for a specific qualification.

Further information on levels and application of sanctions can be found in the AQA Centre Administration Guide for Technical and Vocational Qualifications.
15 Internal assessment and quality assurance

15.1 Overview

The Foundation Technical Level (360 GLH) in IT: Cyber Security (TVQ01010) qualification units K/507/6427 (Developing and maintaining computer networks) and A/507/6433 (Network threats and vulnerabilities) are internally assessed by the centre.

For the Technical Level (720 GLH) in IT: Cyber Security and Security Administration (TVQ01009) qualification units R/507/6437 (Maths for computing), Y/507/6438 (Managing identity and access to systems), D/507/6439 (Programming for networking and security) and/or R/507/6440 (Computer forensic investigation) are internally assessed by the centre.

All assessment decisions that are made internally within a centre are externally quality assured by AQA. AQA has worked with employers and professional bodies to produce guidance on what is the most appropriate form of assessment or evidence gathering for all internal centre assessment.

The most appropriate method of assessment (or evidence gathering) is detailed against each unit. Should a centre wish to use an alternative method of assessment to that detailed, then justification must be provided during AQA quality assurance visits to the centre.

This justification needs to lay out why the centre feels their approach to assessment is more appropriate, efficient or relevant to the learner and/or subject and should be provided in writing to the AQA external quality assurer.

Centres should tailor the assessment to suit the needs of the learner, and internal assessments can take place at a time to suit the centre or learner.

Centres should take a best practice approach with learners being assessed through real life or work-based activity to generate the required evidence (see Section 8.1 Meaningful employer involvement).

15.2 Role of the assessor

The role of the assessor is to:

- carry out initial assessments of learners to identify their current level of skills, knowledge and understanding and any training or development needs
- review the evidence presented against the requirements of the qualification, to make a judgement on the overall competence of learners
- provide feedback to learners on their performance and progress. This feedback needs to give learners a clear idea of the quality of the work produced, where further evidence is required and how best to obtain this.
15.3 **Assessor qualifications and experience**

In order to assess learners working towards this qualification, assessors must:

- have appropriate knowledge, understanding and skills relevant to the units within this qualification
- have experience as a practitioner and/or teaching and training with significant experience of creating programmes of study in relevant subject areas
- undertake activities which contribute to their continuing professional development (CPD).

15.4 **Applying portfolio assessment criteria**

When assessing learner’s work, the centre should consider the level of attainment in four broad areas:

1. the level of independence and originality
2. the depth and breadth of understanding
3. the level of evaluation and analysis
4. the level of knowledge, skills or competency demonstrated.

15.5 **Authentication of learner work**

The centre must be confident that a learner’s work is their own. You must inform your learners that to present material copied directly from books or other sources such as the internet, without acknowledgement, will be regarded as deliberate deception. This also includes original ideas, as well as the actual words or artefacts produced by someone else.

Learners’ work for assessment must be undertaken under conditions that allow the centre to authenticate the work. If some work is done unsupervised, then the centre must be confident that the learners’ work can be authenticated with confidence – eg being sufficiently aware of an individual learner’s standard and level of work to appreciate if the evidence submitted is beyond the level of the learner.

The learner is required to sign a declaration that the work submitted for assessment is their own. The centre will also countersign this declaration that the work was carried out under any specified conditions – recording details of any additional assistance. This must be provided with the learner’s work for external quality assurance purposes.

Any assistance given to an individual learner beyond that given to the group as a whole, even if within the parameters of the specification, must also be recorded.

If some work is done as a part of a team, the centre must be confident that the learner’s contribution to that team activity can be clearly identified and authenticated.

15.6 **Tutor assistance and feedback**

Whilst learners are undertaking assignment tasks, tutors must ensure that any assistance given, or offered as a result of a learner’s question and/or request for help, does not compromise the learner’s ability to independently perform the task in hand.

During assessment, tutors can give general feedback and support to learners, most notably, on the following:

- development of the required knowledge and skills underpinning the assignment at hand
- confirmation of the assessment criteria being assessed
- clarification of the requirements of the Assignment brief
- identification of assignment deadlines.
Tutors, however, must **not** assist learners directly and specifically with assignment tasks.

Tutors are not permitted to provide ‘formative’ feedback on learner’s work, i.e. feedback, prior to submission for marking, on an assignment/task that will enable the learner to amend the assignment/task to improve it.

Once learner work has been submitted for marking, then tutors must give clear and constructive feedback on the criteria successfully achieved by the learner. Tutors should also provide justification and explanation of their assessment decisions. Where a learner has not achieved the performance criteria targeted by an assignment, then feedback should not provide explicit instructions on how the learner can improve their work to achieve the outstanding criteria. This is to ensure that the learner is not assisted in the event that their work is considered for resubmission.

### 15.7 Research and references

Where learners are required to undertake research towards the completion of a task, they should reference their research results in a way that is informative, clear and consistent throughout their work. We do not prescribe a specific way to organise references, but we expect tutors to discuss this with learners and identify a ‘house style’ that learners are then expected to use. Learners may include a bibliography of relevant sources on larger assignments where there has been significant research and there is value in recording all sources fully.

### 15.8 Role of the internal quality assurer

An internal quality assurer (IQA) must be appointed to ensure the quality and consistency of assessments within the centre. Each assessor’s work must be checked and confirmed by an internal quality assurer.

The IQA must observe assessors carrying out assessments, review assessment decisions from the evidence provided and hold standardisation meetings with the assessment team to ensure consistency in the use of documentation and interpretation of the qualification requirements.

All assessment decisions made within a centre must be standardised to ensure that all learners’ work has been assessed to the same standard and is fair, valid and reliable.

Evidence of all standardisation activity should be retained by the centre and could take the form of, for example, records of training or feedback provided to assessors, minutes of meetings or notes of discussions.

Our external quality assurers (EQAs) will always be happy to provide guidance and assistance on best practice.

Internal standardisation activity may involve:

- all assessors marking trial pieces of work and identifying differences in marking standards
- discussing any differences in marking at a training meeting for all assessors
- cross-moderation of work between assessors.
15.9 Internal quality assurer qualifications and experience

In order to internally quality assure the assessment of learners working towards this qualification, IQAs must:

• have appropriate knowledge, understanding and skills relevant to the units within these qualifications
• have experience as a practitioner and/or teaching and training with significant experience of creating programmes of study in relevant subject areas
• undertake activities which contribute to their continuing professional development (CPD).

15.10 Record keeping

The centre must be able to produce records that show:

• the assessor and IQA allocated to each learner
• the evidence assessed
• the dates of assessment and IQA
• details of internal standardisation activities of the assessor – (what, when and by whom)
• the grade awarded and rationale for this.
16 Resits, resubmissions and retakes

16.1 Note on terminology

**Resits** refer to learners taking further attempts at an examined/externally assessed unit.

**Resubmissions** refer to learners undertaking a second attempt at an internally assessed unit task/assignment prior to external quality assurance.

**Retakes** refer to learners undertaking a second attempt at an internally assessed unit after external quality assurance.

16.2 Rules on resits, resubmissions and retakes

Resits and retakes are permitted where a learner has either failed the requirements of the unit, or where they wish to improve on a grade awarded.

For certification purposes, AQA will recognise the best achievement by the learner and not the most recent.

**Resitting an exam or external assessment**

The learner is permitted **three** attempts (one initial and two resits) in relation to each examined/externally assessed unit of the specification.

Learners who have been awarded the Foundation qualification and have progressed to the full Technical Level are allowed to use the resit opportunities to go back and improve the grade achieved in the external assessment. Any improvement cannot be used to upgrade and reclaim the previously awarded Foundation qualification.

**Resubmitting internal assessments**

The learner is permitted **one** resubmission in relation to each internally assessed unit of the qualification, but only when the tutor believes the learner can achieve the outstanding criteria without further guidance. Any resubmission of work must be undertaken prior to external moderation.

**Retaking internal assessments**

The learner is permitted **one** retake in relation to each internally assessed unit of the qualification. This could mean the learner doing the entire unit work again, or simply correcting a task/assignment before the unit is again submitted for external moderation by AQA. With a retake, learners are not allowed a resubmission opportunity.

Any retake and/or resubmission of work must be completed within a defined and reasonable period of time following learner feedback of the initial assessment. Any work provided as evidence must be authenticated by the learner as their own.
17 Grading

17.1 Overview

Performance in all units is graded at Pass, Merit or Distinction. These unit grades are then converted into points and added together to determine the overall grade for the qualification.

The overall Foundation Technical Level in IT: Cyber Security (TVQ01010) qualification is graded as P, M, D, D*.

The overall Technical Level in IT: Cyber Security and Security Administration (TVQ01009) qualification is graded as PP, MP, MM, DM, DD, D*D, D*D*.

17.2 Internally assessed units

Centres must ensure that all assessment criteria in the unit are covered during the teaching and learning process so that learners can meet the requirements. Work should be assessed against the grading criteria provided within each unit.

• To achieve a Pass, a learner must have satisfied all Pass criteria.
• To achieve a Merit, a learner must achieve all of the Pass and all of the Merit criteria.
• To achieve a Distinction, a learner must achieve all of the Pass, Merit and Distinction criteria.

17.3 Externally assessed (examined) units

These units are assessed by AQA using a marks-based scheme. After the assessment has taken place and been marked, the grade boundaries are set by AQA. These grade boundaries are based on the level of demand of the assessment and learners’ performance – all learners that took the assessment, not just those in your centre.

When the assessment results are shared with the centre, AQA will report on the grade boundaries.

Note: These grade boundaries may change for each assessment window according to the demand of the assessment – this is important to maintain standards across each window.

Learners’ grades are converted into points.

17.4 Points per grade – unit level

Table 1 shows the points for each grade at a unit level.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Internally/centre assessed unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>36</td>
</tr>
<tr>
<td>Merit</td>
<td>54</td>
</tr>
<tr>
<td>Distinction</td>
<td>72</td>
</tr>
</tbody>
</table>
17.5 Final grade for overall qualification

The total possible number of points that can be achieved for the Foundation Technical Level (360 GLH) in IT: Cyber Security is 288.

The total possible number of points that can be achieved for the Technical Level (720 GLH) in IT: Cyber Security and Security Administration is 576.

Points for overall qualification grade

Table 2: Foundation Technical Level (360 GLH) in IT: Cyber Security (TVQ01010)

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points boundary</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>144</td>
</tr>
<tr>
<td>M</td>
<td>198</td>
</tr>
<tr>
<td>D</td>
<td>252</td>
</tr>
<tr>
<td>D*</td>
<td>270</td>
</tr>
</tbody>
</table>

Table 3: Technical Level (720 GLH) in IT: Cyber Security and Security Administration (TVQ001009)

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points boundary</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP</td>
<td>288</td>
</tr>
<tr>
<td>MP</td>
<td>360</td>
</tr>
<tr>
<td>MM</td>
<td>396</td>
</tr>
<tr>
<td>DM</td>
<td>468</td>
</tr>
<tr>
<td>DD</td>
<td>504</td>
</tr>
<tr>
<td>D*D</td>
<td>522</td>
</tr>
<tr>
<td>D<em>D</em></td>
<td>540</td>
</tr>
</tbody>
</table>

17.6 The ‘Near Pass’ rule

A near pass will be applied to an externally assessed unit for those learners who may fall just short of a pass grade. The unit grade will still be reported as a grade U, since the learner will not have performed to the minimum standard required for a Pass grade, but will qualify as a near pass for the purposes of determining the overall qualification grade.

The actual mark required to achieve the ‘near pass’ grade on an examined unit will change from year to year, depending on the grade boundaries that have been set. A learner will receive 27 points if they achieve a Near Pass.

A learner is allowed one Near Pass in an externally assessed unit in a Foundation Technical Level or up to two Near Pass results (six or eight unit Technical Level) or up to three Near Pass results (12 unit Technical Level).

All other eligibility requirements for achieving the qualification will remain the same:
- the total points score is above the Pass threshold; and
- all other units are passed
18 Administration arrangements

Full details of all of the administration arrangements relating to AQA Tech-levels can be found in the AQA Centre Administration Guide for Technical and Vocational Qualifications, including:

- how to apply for centre approval
- registration of learners
- dealing with recognition of prior learning (RPL)
- how to make examination entries
- dealing with missed examination dates
- examination invigilation arrangements
- how to make claims for certificates
- how to appeal against an assessment, IQA or EQA decision
- retention of learner work and assessment/IQA records
- dealing with potential malpractice or maladministration.

Details of all AQA fees can be found on the AQA website at aqa.org.uk
19 Appendix A: Transferable skills standards and guidance

19.1 Transferable skills – communication standards (oral)

Evidence must clearly show that the learner can:

| CO1 | Prepare a suitable presentation. | 1.1 Research suitable topics for the presentation. |
|     |                                 | 1.2 Research the most appropriate format for the presentation. |
|     |                                 | 1.3 Plan the structure of the presentation. |
|     |                                 | 1.4 Make use of any appropriate supporting materials and prepare any other resources needed for the presentation. |

| CO2 | Use language, vocabulary, tone and style suited to the complexity of the topic and the context. | 2.1 Use appropriate language and vocabulary. |
|     |                                               | 2.2 Structure what is presented to help the audience follow the sequence of the main points and ideas. |
|     |                                               | 2.3 Use tone and style of presentation appropriate to the audience and environment. |

| CO3 | Use a variety of methods to engage the audience. | 3.1 Provide examples to illustrate complex points. |
|     |                                               | 3.2 Use relevant images from appropriate sources to illustrate key points. |
|     |                                               | 3.3 Use at least one additional method to engage the audience. |

Required evidence
- Learner preparation evidence (planning notes, research).
- Learner presentation including all support materials.
- Assessor observation record.

Learner guidance
The learner should consider the purpose, topic and audience as follows:
- the presentation should be eight minutes long to allow the learner to demonstrate the appropriate skills
- the presentation must always be contextualised within the technical subject content, and should not be simulated
- an audience of at least two or three people which may or may not include peers.

For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
CO1
There should be evidence showing that the learner has:
• researched the technical subject content of a complex matter
• selected information relevant to the purpose of the presentation
• planned how to structure the presentation
• planned to use a relevant image or images to illustrate key points of the presentation – that adds value to the overall presentation
• included one additional method to engage audience for example questioning, completion of hand-out, discussion etc.

CO2
Learners should:
• give a well-structured delivery and must clearly highlight the main points of their presentation using tone, gesture or expression
• use appropriate vocabulary suited to the audience and environment.

CO3
Learners must:
• give examples to explain ideas
• make effective use of an image or images and other support materials to engage the audience and to illustrate key points, for example through use of video clips, explanatory notes or other technically related activities.

Tutor guidance
• Tutors should use an observation record to support their assessment.
• Tutors should ensure that those observing are familiar with the observation record content and purpose.
• The presentation may be delivered through spoken communication or using sign language.
• Tutors should look for fitness of purpose and styles of presentation. Brief notes may be used as a prompt, but learners should not rely on them entirely.
19.2 Transferable skills – communication standards (written)

Evidence must clearly show that the learner can:

| CW1 | Select appropriate formats for presenting information as a report. | 1.1 Decide on the most appropriate format for the technical report.  
1.2 Plan the structure of the technical report.  
1.3 Make use of any appropriate supporting materials and prepare any other resources needed for the technical report. |
| CW2 | Select and use an appropriate style and tone to suit their audience. | 2.1 Use appropriate language and vocabulary.  
2.2 Structure the technical report to help the audience follow the sequence of the main points and ideas.  
2.3 Use tone and style appropriate to the intended recipient(s). |
| CW3 | Organise material coherently, to suit the length, complexity and purpose of their technical report, proofread and where necessary, re-draft documents. | 3.1 Spell, punctuate and use grammar accurately.  
3.2 Make their meaning clear.  
3.3 Use relevant images from appropriate sources to illustrate key points.  
3.4 Proofread their technical report.  
3.5 Obtain feedback and amend technical report accordingly. |

Evidence required

- A learner technical report of at least 1,000 words excluding support materials.
- An assessor recording form*.

Learner guidance

The learner should:

- produce a technical report about a complex subject which must be at least 1,000 words long
- include subject matter, which may well have a number of strands that is challenging to the individual learner in terms of the ideas it presents.

---

* For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills

Visit aqa.org.uk for the most up-to-date specification, resources, support and administration
CW1
It is essential that learners know how to:
• organise their technical report
• link paragraphs in various ways
• use features, such as indentation and highlighting, to suit different types of documents.

CW2
Learners should know how to:
• produce a technical report that takes account of the vocabulary, tone and techniques normally used when producing documents for particular purposes and different recipients
• write with confidence and with the appropriate degree of formality.

CW3
In supporting key points:
• images that could be used include: graph, sketch, picture or material taken from a presentation
• learners should know how to check their work to ensure that spelling, punctuation and grammar are accurate
• learners should know how to write grammatically correct sentences, including correct use of a variety of verb tense, form and person (for example passive voice); spell accurately, complex, irregular and technical words and use punctuation effectively for example bullet points, semicolon, colon, apostrophes) to ensure their meaning is clear.

Tutor guidance
For the technical report produced, assessors should look for evidence that the learner has:
• selected an appropriate format for report
• organised relevant information using a clear and coherent structure
• used technical vocabulary when appropriate
• ensured that text is legible with accurate use of spelling, grammar and punctuation.

The learner should not be penalised for one or two errors providing meaning is still clear.
19.3 Transferable skills – problem-solving standards

Evidence must clearly show that the learner can:

| PS1 | Identify a problem and the tools and techniques that could be used to explore the problem. | 1.1 Identify, analyse and describe the problem.  
1.2 Identify a variety of tools and techniques which could be used to explore the problem.  
1.3 Plan how you will investigate the problem highlighting which tools and techniques will be used. |
| PS2 | Implement both the plan to investigate the problem and the plan to solve the problem. | 2.1 Implement the plan for investigating the problem and seek support and feedback from others as necessary.  
2.2 Record and analyse the results of the investigation.  
2.3 Identify the solution(s) to solve the problem.  
2.4 Plan the steps to be taken in order to solve the problem, identifying any risks, and implement the solution. |
| PS3 | Check if the problem has been resolved and review the approach to tackling problems. | 3.1 Check whether the problem has been resolved/solved.  
3.2 Analyse the results and draw conclusions on the success of the problem-solving process.  
3.3 Review the approach to tackling/solving the problem, including whether other approaches might have proved more effective. |

Evidence required

- Explore/plan* – to be completed by the learner.
- Do* – to be completed by the assessor.
- Review* – to be completed by the assessor.

Learner guidance

The learner must demonstrate:

- a systematic approach to tackling problems, including identifying which is the most appropriate method, then developing a plan and implementing it
- how they went about the problem-solving process.

Evidence should be on individual performance. A group approach to problem-solving does not allow learners to achieve specific elements of the standards.

Activities must always be in relation to the core subject content and should not be simulated.

Effective definition of the problem will help the learner tackle it systematically and produce valid evidence. Tutors may discuss with learners the most appropriate definition of the problem and what sort of results might be expected so the learner is clear on what would show that the problem had been solved.

---

10 For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills
**PS1**

Learners should:
- recognise, identify and describe the main features of the problem
- identify how they will explore the problem and the tools and techniques they will use
- use a variety of methods for exploring the problem.

**PS2**

Learners should:
- obtain approval to implement their plan from an appropriate person, which could be the tutor or supervisor
- make effective judgements, based on feedback and support available, when putting their plan into action
- check their plan regularly for progress and revise it accordingly.

**PS3**

Learners should:
- use an appropriate method for checking if the problem has been solved. For example if a learner designed a procedure or process for improving a system that records information, they would need to test this out and report back on their findings
- know how to describe the results in detail and draw conclusions on the success of their problem-solving skills
- reflect back on the process considering areas such as:
  - did they spend enough time considering the features of the problem?
  - were they effective in planning action points to tackle the problem?
  - did they take a logical approach to checking if the problem had been solved/resolved?

In some circumstances, achievement of the standard may be possible even if the problem has not been solved or resolved, especially if factors were outside of their control, and the learner was able to demonstrate the process of tackling the problem.

**Tutor guidance**

- Tutors should check problem-solving implementation planning.
- Tutors may be required to provide a witness statement in support of evidencing the processes.
19.4 Transferable skills – research standards

Evidence must clearly show that the learner can:

| R1 | Design a research study. | 1.1 Identify possible topics for research.  
1.2 Choose one topic, identifying appropriate objectives for detailed research, and plan how to carry out the research.  
1.3 Select a variety of resources to gather relevant information and identify appropriate methods and techniques to carry out the research. |
| R2 | Conduct data collection and analysis. | 2.1 Collect data using the appropriate methods to test the hypotheses/theories.  
2.2 Carry out an appropriate analysis of the data.  
2.3 Draw appropriate conclusions that are supported by the evidence from the data analysis. |
| R3 | Present findings of the research and evaluate the research activities. | 3.1 Prepare and present results of research.  
3.2 Present the information in a clear and appropriate format adapted to the needs of the audience.  
3.3 Seek feedback and use it to support own evaluation of research skills. |

Required evidence

- Plan* – to be completed by the learner.
- Do* – to be completed by the assessor.
- Review* – to be completed by the assessor.
- Results of research.

Learner guidance

The learner should demonstrate they can:

- identify clear and appropriate objectives for the research study
- plan and carry out research activities with the particular objectives in mind
- design their research study in a systematic way
- present their findings as well as evaluating their research skills and activities
- be clear about the objectives of the research study, for example to assess the positive and negative impact of digital photography on sports journalism to predict future trends
- identify sources, methods and strategies they plan to use to investigate the topic
- carry out the research within a clearly defined structure, with a measure of complexity that should be reflected in the breadth and nature of the research objectives
- undertake the analysis required to make the best use of information/data and the requirement to give a clear justification for their conclusions
- make different research methodologies.

Activities must always be contextualised within the core subject content, and should not be simulated.

¹¹ For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills
RS1
The learner should explore:
• a variety of possible topics to research and should spend time deciding on clear and measurable objectives when designing their research study
• objectives and discuss and agree them with a tutor or supervisor
• a wide variety of sources when gathering their information
• the use of at least three different types of resource
• one source that is primary (gathered by the learner), for example, interview, questionnaire, survey, rather than from secondary for example encyclopaedia, interpretations of original material.
The learner should produce a plan detailing how they will carry out the research.

RS2
The learner should:
• keep a record of the sources used
• independently collect information including data
• analyse information collected and identify information and data most relevant to their research objectives.

RS3
When presenting their findings, learners should:
• use a format that is most appropriate to the content in terms of audiences, subject matter and research objectives
• communicate research findings clearly
• seek feedback from appropriate people
• show how they have used this feedback to help evaluate their research skills
• evaluate their research activities addressing all aspects including identifying the research objectives, collecting and analysing data and/or information, and recording, presenting and explaining findings.

Tutor guidance
• Tutors should agree research objectives with learner.
• Tutors should check that different types of resource have been used.
19.5 Transferable skills – teamwork standards

Evidence must demonstrate the learner can:

| TW1   | Plan the work with others. | 1.1 Agree realistic objectives for working together and what needs to be done in order to achieve them. |
|       |                            | 1.2 Share relevant information to help agree team roles and responsibilities. |
|       |                            | 1.3 Agree suitable working arrangements with other team members. |
| TW2   | Develop and maintain cooperative ways of working towards agreed objectives checking progress on the way. | 2.1 Organise and complete own tasks efficiently to meet responsibilities. |
|       |                             | 2.2 Seek effective ways to develop cooperation such as ways to resolve conflict and maintain open communication. |
|       |                             | 2.3 Share accurate information on progress and agree changes where necessary to achieve objectives. |
| TW3   | Review working with others and agree ways of improving collaborative work in the future. | 3.1 Agree the extent to which working with others has been successful and objectives have been met. |
|       |                             | 3.2 Identify factors, including their own role, in influencing the outcome. |
|       |                             | 3.3 Provide details of how they could improve working with others in the future, including interpersonal skills. |

A group/team is defined as three or more people (eg peer, co-worker) who are working towards shared objectives. It is not acceptable for tutors/assessors to be part of the team. The nature of the teamworking should reflect the sector in which the qualification sits, eg engineering, business or IT.

Required evidence¹²

- Plan*.
- Do*.
- Review*.
- Minutes of meetings.
- Witness statement.
- Peer statements.

Learner guidance

Meeting the standard will confirm that the learner has:

- demonstrated the ability to work cooperatively with others
- be clear about the objectives the team or group is working towards and their own responsibilities
- planned and carried out the work supporting others, reviewing outcomes and suggesting ways of improving work with others.

Activities must always be contextualised within the core subject content, and should not be simulated.

¹² For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills
TW1
As part of the initial team planning meeting the learner should:
• offer suggestions and listen to others to agree realistic objectives, prioritise tasks and identify resources and timescales
• be clear about their own responsibilities and the areas of work for which they are answerable to others
• produce a plan showing what needs to be done by the team clarifying own responsibilities and arrangements for working with others in the team.

TW2
Learners should take responsibility for:
• organising their own work to meet the agreed deadlines
• the use of correct and appropriate techniques and approaches when carrying out tasks
• actively looking for ways to develop and support cooperative working, including helping to deal with conflict and taking a lead role in anticipating the needs of others
• considering the rights and feeling of others
• ensuring at least one team progress meeting should be held before the final review meeting.

TW3
During the team review meeting learners should:
• provide information about their own contribution to the work of the team ie what did they do and how did they interact with other members of the group
• explain how improved inter-personal skills could contribute to more effective collaboration in the future (for example ‘I should listen more carefully when negotiating activities/tasks’)
• identify improvements they could make in managing tasks (for example ‘I could have been better organised with notes at team meetings’).

Tutor guidance
Tutors are encouraged to support the evidence process by completing a witness statement.
Get help and support

Visit our website for information, guidance, support and resources at aqa.org.uk/tech-levels

E: techlevels@aqa.org.uk

T: 0800 085 0391

LEVEL 3 FOUNDATION TECHNICAL LEVEL
IT: CYBER SECURITY
360 GLH (TVQ01010)

LEVEL 3 TECHNICAL LEVEL
IT: CYBER SECURITY AND SECURITY ADMINISTRATION
720 GLH (TVQ01009)

Specifications
First registration September 2015 onwards

Version 3.1 November 2018