AQA
Realising potential

LEVEL 3 FOUNDATION TECHNICAL LEVEL IT: TECHNICAL SUPPORT

360 GLH (TVQ01014)

LEVEL 3 TECHNICAL LEVEL IT: USER SUPPORT

720 GLH (TVQ01012)

Specifications
First registration September 2016 onwards

Version 5.1 November 2018

Contents

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).

2 Qualification at a glance – overview

2.1 Level 3 Foundation Technical Level IT: Technical Support

Ofqual qualification number	601/7126/1	**AQA qualification number**	TVQ01014
First registration date	1 September 2016	**Age range**	16–18, 19+
Last registration date	31 August 2020	**UCAS points**	Information on UCAS points can be obtained from ucas.com
Last certification date	31 August 2023	**Performance table points**	Information on performance measures can be found at education.gov.uk
Total qualification time (TQT)	380 (GLH = 360) (See TQT section for more information)	**Eligibility for funding**	Yes
Unit weighting **Externally assessed** **Internally assessed**	25% each unit (2 x units) 25% each unit (2 x units)	**Entry requirements**	There are no formal entry requirements for this qualification set by AQA.

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.

- Research
- Problem-solving

2.2 Level 3 Technical Level IT: User Support

Ofqual qualification number	601/7130/3	**AQA qualification number**	TVQ01012
First registration date	1 September 2016	**Age range**	16–18, 19+
Last registration date	30 August 2020	**UCAS points**	Information on UCAS points can be obtained from ucas.com
Last certification date	30 August 2023	**Performance table points**	Information on performance measures can be found at education.gov.uk
Total qualification time (TQT)	760 (GLH = 720) (See TQT section for more information)	**Eligibility for funding**	Yes
Unit weighting **Externally assessed** **Internally assessed**	12.5% each unit (3 x units) 12.5% each unit (5 x units)	**Entry requirements**	There are no formal entry requirements for this qualification set by AQA.

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 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.

- Research
- Problem-solving
- Communication (oral)
- Teamwork

3 Level 3 Foundation Technical Level IT: Technical Support: 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: Technical Support

- 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 support job roles in a variety of sector settings, or as the first year of a two year programme where learners aspire to achieve the IT: Networking or IT: User Support qualifications.

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: Scripting and App Programming or the IT: Programming qualification 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 of the units in this qualification are mandatory and will provide a core knowledge and understanding of IT: technical support. Focusing on computer networks and supporting end users to solve computer and network related issues, all based on underpinning units in the fundamental principles of computing and communication technologies, this 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 which they use
- designing and developing a simple computer network from a user specification and creating a maintenance plan
- fault investigation, diagnosis and resolution
- how to provide a service to technology users.

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
- problem-solving.

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

Unit code	Unit title	Transferable skill(s)
K/507/6427	Developing and maintaining computer networks	Research
M/507/6428	Supporting end users	Problem-solving

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, as a junior IT support technician. Learners would have an opportunity for further study, topping up this qualification to a Level 3 Technical Level in IT: Networking or IT: User Support qualification. This qualification will also contribute to university entry and will provide opportunities to undertake a range of professional qualifications from vendors such as 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, the Extended Project Qualification (EPQ), an AS and possibly re-sits for English and/or Maths GCSE, 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 technician, network technician, computer maintenance technician, helpdesk operator.

Companies that might employ someone with this qualification are:

- 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:

bcs The Chartered Institute for IT	British Computer Society (BCS)	bcs.org
TECH PARTNERSHIP	The Tech Partnership	thetechpartnership.com
UK Cyber Security Forum	UK Cyber Security Forum	ukcybersecurityforum.com
D-RISQ SOFTWARE SYSTEMS	D-RisQ	drisq.com
fasthosts Inspiring Better Business	Fasthosts	fasthosts.co.uk
TOSHIBA Leading Innovation	Toshiba UK	toshiba.co.uk
NETGEAR®	NETGEAR	netgear.co.uk

	Weheartdigital Limited	weheart.digital
	CompTIA	comptia.org
	Microsoft	microsoft.com
	AlfaPeople UK	alfapeople.com
	RSPCA	rspca.org.uk
	CCL Group Limited	cclgroupltd.com
	Cisco	cisco.com
	VMWare IT Academy	vmware.com
	Axelos	axelos.com
	City of Wolverhampton College	wolvcoll.ac.uk
	Burton and South Derbyshire College	bsdc.ac.uk

Solihull College & University Centre	Solihull College	solihull.ac.uk
SOUTH & CITY COLLEGE BIRMINGHAM	South and City College Birmingham	sccb.ac.uk
NULC Newcastle-under-Lyme College	Newcastle-under-Lyme College	nulc.ac.uk
Edge Hill University	Edge Hill University	edgehill.ac.uk
University of Bedfordshire	University of Bedfordshire	beds.ac.uk or beds.ac.uk/howtoapply/departments/teacher-education/tt
STAFFORDSHIRE UNIVERSITY	Staffordshire University	staffs.ac.uk

3.6 What are the benefits of this qualification?

To learners

People often forget how much organisations and businesses in the United Kingdom, Europe and around the world in general, rely on IT technical support staff keeping computer systems and networks operational. Most businesses could not trade in the modern economy without technicians ensuring that computers and devices linked to them are working.

Studying this qualification will give you a variety of options. You could choose to use your achievements to contribute towards the larger IT: Networking or IT: User Support qualifications 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 to build and maintain a computer, build and maintain a network and to help and support other users. 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 which 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 which 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.

Beginning with the fundamental principles of computing, you will study how computers and devices communicate, how networks are built and maintained and you will understand 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 or entry 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 and skills in problem-solving, which are important sector skills.

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 support end users.

Employers can therefore be confident that learners have a solid technical IT grounding and personal skills in research and problem-solving.

To higher education institutions

Discussions with higher education institutions (HEIs) during the development of this IT: Technical Support 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 and problem-solving skill development.

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

In this qualification learners will build on the fundamental principles of computing, they will study how computers and devices communicate, how networks are built and maintained and they will understand how to support other users.

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).

4 Level 3 Foundation Technical Level IT: Technical Support: Unit summary

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

	Unit title	Assessment type	Ofqual unit reference
1	Fundamental principles of computing	External examination	Y/507/6424
2	Communication technologies	External examination	H/507/6426
3	Developing and maintaining computer networks	Internally centre assessed	K/507/6427
4	Supporting end users	Internally centre assessed	M/507/6428

Links with other qualifications

The following units are 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: Cyber Security and IT: Cyber Security and Security Administration:

H/507/6426 2 Communication technologies
K/507/6427 3 Developing and maintaining computer networks

The following units are shared with IT: Networking and IT: User Support:

M/507/6428 4 Supporting end users

5 Level 3 Technical Level IT: User Support: 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 these areas:

AQA Level 3 Technical Level IT: User Support

- 3132 – IT user support technician
- 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 junior user support, IT technician, or helpdesk operator job roles in a variety of sector settings, or an IT user support 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 Scripting and App programming, or vendor qualifications such as Cisco, Oracle, CompTia, VMWare or LPI for those who seek a role in related disciplines such as telecommunications or database administration and support.

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?

All of the units in this qualification are mandatory and will provide a core knowledge and understanding of IT user support.

Focusing on concepts such as troubleshooting, testing, installation and maintenance of software, system security and forensic analysis and, built on core learning in this sector through the fundamental principles of computing unit and communication technologies, this 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 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
- fault investigation, diagnosis and resolution
- how to provide a service to technology users
- software and hardware installation and upgrading
- forensic investigation based on analytical and investigative techniques to examine digitally stored or encoded information, used in the detection and prevention of crime
- computer security and how internal and external threats can be managed
- physical security including devices such as secureID tabs and biometrics
- contractual and legal issues around the use of IT.

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)
- research
- teamwork
- problem-solving.

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

Unit code	Unit title	Transferable skill(s)
A/507/6464	Industrial project	Teamwork
R/507/6440	Computer forensic investigation	Communication (oral)
K/507/6427	Developing and maintaining computer networks	Research
M/507/6428	Supporting end users	Problem-solving

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 at 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 into work in a technical support role in areas such as: helpdesk, customer support, systems support, building computers, fault finding, support and repair. Learners would have an opportunity for further study either through university or through professional qualifications from a range of vendors.

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, the Extended Project Qualification (EPQ), an AS and possibly re-sits for English and/or Maths GCSE, 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:

- customer support analyst, helpdesk operator, IT support technician, systems support officer, IT technician, network administrator, systems administrator.

Companies that might employ someone with this qualification are:

- any company seeking technical support staff, 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:

bcs The Chartered Institute for IT	British Computer Society (BCS)	bcs.org
TECH PARTNERSHIP	The Tech Partnership	thetechpartnership.com
UK Cyber Security Forum	UK Cyber Security Forum	ukcybersecurityforum.com
D-RISQ SOFTWARE SYSTEMS	D-RisQ	drisq.com
fasthosts Inspiring Better Business	Fasthosts	fasthosts.co.uk

	Toshiba UK	toshiba.co.uk
	NETGEAR	netgear.co.uk
	Weheartdigital Limited	weheart.digital
	CompTIA	comptia.org
	Microsoft	microsoft.com
	AlfaPeople UK	alfapeople.com
	RSPCA	rspca.org.uk
	CCL Group Limited	cclgroupltd.com
	Cisco	cisco.com
	VMWare IT Academy	vmware.com
	Axelos	axelos.com

	City of Wolverhampton College	wolvcoll.ac.uk
	Burton and South Derbyshire College	bsdc.ac.uk
	Solihull College	solihull.ac.uk
	South and City College Birmingham	sccb.ac.uk
	Newcastle-under-Lyme College	nulc.ac.uk
	Edge Hill University	edgehill.ac.uk
	University of Bedfordshire	beds.ac.uk or beds.ac.uk/howtoapply/departments/teacher-education/tt
	Staffordshire University	staffs.ac.uk

5.6 What are the benefits of this qualification?

To learners

User support is an often busy and sometimes complex environment, but would be a good career choice for those who want to work in a technical role but who would also enjoy working with end users. These could be commercial customers or just those who work within an organisation, or sometimes both, but the key to success in this role is the ability to communicate in a variety of situations and do so in a professional way. Technical staff in such a role should always remember that they are the public face of the department and the company itself.

Learners should be prepared to undertake research when solving IT problems, finding the best solution for the user, which could be simple advice, or could require more technical information that would need to be gathered from a variety of sources. For example, learning how to engage in technical conversations and following the threads of a discussion can be very useful in finding the right solution for your user.

Studying this qualification as part of a learning programme could include study in other areas also, which will help you to develop the skills and knowledge that are needed in the fast-moving IT sector.

You will be working on industry-focussed assignments to help you to prepare for work which 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 HE colleges 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, you will understand network security, how to install and maintain software and how to support end users.

With experience you might be able to specialise hardware, security or software support in a variety of roles such as systems administrator, helpdesk operator and eventually you would be well placed to move into a management role.

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 work 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 teamwork, the ability to research, skills in problem-solving and in both written and oral communication.

Building on the fundamental principles of computing, learners will have studied how computers and devices communicate, how networks are built and maintained, how software should be maintained, they will understand operational security and how to support end users. In addition learners will have forensically explored computer systems and be ready to support users at a basic level.

All learners will have been involved in a contextualised project that will have been industry driven and that will demonstrate the ability to contribute to team performance.

Employers can therefore be confident that learners have a comprehensive grounding in technical and personal skills.

To higher education institutions

Discussions with higher education institutions (HEIs) during the development of this user support qualification identified that to succeed in higher study in this area, learners should understand the concepts of customer service in an IT role. Communication skills should have been developed to ensure competence in both the written and spoken context.

In addition, learners will have built on the fundamental principles of computing, learners will have studied how computers and devices communicate, how networks are built and maintained, they will understand network security and how to support end users.

All learners will have been involved in a contextualised project that will have been industry driven and that will demonstrate the ability to contribute to team performance.

HEIs can therefore be confident that learners will be ready to study at higher levels.

5.7 Links to trailblazers

At this stage there is no User Support Trailblazer – however, as some of the units are Network related, this could provide the opportunity to progress to a Level 4 Trailblazer Apprenticeship as a Network Engineer: apprenticeships.org.uk/~/media/Apprenticeship-standards/DI%20-%20Network.ashx

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: User Support: Unit summary

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

	Unit title	Assessment type	Ofqual unit reference
1	Fundamental principles of computing	External examination	Y/507/6424
2	Communication technologies	External examination	H/507/6426
3	Developing and maintaining computer networks	Internally centre assessed	K/507/6427
4	Supporting end users	Internally centre assessed	M/507/6428
5	Installing and maintaining software	Internally centre assessed	M/507/6493
6	Organisational systems security	External examination	T/507/6494
7	Computer forensic investigation	Internally centre assessed	R/507/6440
8	Industrial project	Internally centre assessed	A/507/6464

Links with other qualifications

The following units are shared across the IT sector:

Y/507/6424 1 Fundamental principles of computing

The following unit is shared with the IT: Networking and IT: Programming:

A/507/6464 8 Industrial project

The following units are shared with IT: Cyber Security, IT: Technical Support, IT: Networking, IT: User Support and IT: Cyber Security and Security Administration:

H/507/6426 2 Communication technologies
K/507/6427 3 Developing and maintaining computer networks

The following units are shared with IT: Networking and IT: User Support:

M/507/6428 4 Supporting end users

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 (MEI) 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:

- gov.uk/government/uploads/system/uploads/attachment_data/file/306280/RR341_-_Employer_Involvement_in_Qualifications_Delivery_and_Assessment_Research_Report.pdf
- gov.uk/government/uploads/system/uploads/attachment_data/file/268624/document.pdf

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:

Unit	Assessment outcomes/ pass criteria	Synoptic links to other units	% of synoptic assessment
Fundamental principles of computing	5	Underpinning knowledge for sector	5/5 (100%)
Communication technologies	5	Underpinning knowledge for pathway	5/5 (100%)
Developing and maintaining computer networks	14	Linked to Units 1, 2, 4, 5, 6, 7 and 8	9/14 (64%)
Supporting end users	16	Linked to Units 1, 3, 5 and 8	16/16 (100%)
Installing and maintaining software	13	Linked to Units 1, 4, 6 and 8	9/13 (69%)
Organisational systems security	4	Linked to Units 1, 3, 4, 5, 7 and 8	5/5 (100%)
Computer forensic investigation	12	Linked to Units 1, 4, 5, 6 and 8	5/12 (42%)
Industrial project	All units contribute to the industrial project where learners will work together to create solutions for users or a client.		

This qualification contains 71.88% synopticity calculated over all eight units, or 82.1% synopticity calculated over seven units (excluding industrial project).

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:

Qualification	Guided learning hours (GLH)	Total qualification time (TQT)
IT: Technical Support (TVQ01014)	360	380
IT: User Support (TVQ01012)	720	760

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:

- teamworking
- communication (oral and written)
- 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 standard[3]. Not every unit within the qualification has a skill contextualised within the subject content.

Unit code	Pathway	Unit title	Transferable skill(s)
A/507/6464	User Support	Industrial project	Teamwork
R/507/6440	User Support	Computer forensic investigation	Communication (oral)
K/507/6427	Technical Support User Support	Developing and maintaining computer networks	Research
M/507/6428	Technical Support User Support	Supporting end users	Problem-solving

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.

The Transferable skills standards can be found at Appendix A.

[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.

11 Support materials and guidance

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-user-support/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-user-support/assessment-resources

12 Qualification units

12.1 Unit 1: Fundamental principles of computing

Title	Fundamental principles of computing
Unit number	Y/507/6424
Assessment	Externally assessed
Guided learning hours	90
Transferable skill(s) contextualised within this unit	N/A
Resources required for this unit	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.
Synoptic assessment within this unit	This unit provides the underpinning knowledge for all units contained in either the IT: Technical Support or the IT: User Support pathway.

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

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

Hardware components of a computer system	
The internal components of a computer CPU	• Arithmetic logic unit (ALU). • Main memory. • Cache. • Control unit. • Registers; accumulator etc. • The steps of the Fetch-Execute Cycle. • The effect of an interrupt on a Fetch-Execute Cycle. • Pipelines. • Multi-core processors.

Hardware components of a computer system	

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

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

Software requirements of a computer system	
Types of software	• Systems software. • Applications software. • Shareware. • Freeware. • Open source.

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 weakness 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

- Hedly S and Aplin T, *Blackstone's statutes on IT and e-commerce,* 4th edition, ISBN-10 0199238219, ISBN-13 978-0199238217, Blackstone Press (2008).
- Reed C (ed.), *Computer law*, ISBN-10 0199696462, ISBN-13 978-0199696468, Oxford University Press (2012).
- Render B, Stair R and Hanna M, *Fundamentals of information systems*, 7th edition, ISBN-10 1133629628, ISBN-13: 978-1133629627, Mason, OH, South-Western College Publishing, 2013.
- Shelly GB and Cashman TJ, *Computer fundamentals for an information age*, ISBN 0-88236-125-2, Anaheim Publishing Company, Brea, CA, 2013.
- Burdett A, Bowen D, Butler D, Cumming A et al, *BCS glossary of computing and ICT*, ISBN-13 9781780171500 (2013).

Websites

- e-booksdirectory.com (online books for download or reading, some free resources).

12.2 Unit 2: Communication technologies

Title	Communication technologies
Unit number	H/507/6426
Assessment	Externally assessed
Guided learning hours	90
Transferable skill(s) contextualised within this unit	N/A
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: Technical Support linked to Units 1 and 3. IT: User Support linked to Units 1, 3, 6, 7 and 8. This unit provides complementary coverage to Unit 1, the Fundamental principles of computing, by moving the learner beyond a single 'standalone' computer system. Units 3, 6 and 7 all develop data communication concepts introduced in this examining different types of networks, their logical and physical design, uses, security and implementation. Learners will use learning form this unit to underpin their Industrial Project (Unit 8). Extended guidance on synoptic assessment is provided later in this unit documentation.

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, (eg industrial, atmospheric).
	• Error detection and correction techniques, eg:
	  • 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, eg coaxial, unshielded and shielded twisted pair (UTP/STP).
	• Optical.
	• Wireless eg:
	  • 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	

Network topologies	• Different topologies, their key features, strengths and weaknesses:
	  • bus
	  • ring
	  • star
	  • tree
	  • mesh.

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

Network risks	• Hacking and disruption. • Loss of data. • Loss of service. • Loss of income. • Compromise of data integrity. • Loss of reputation; commercial damage.

Network conceptual models, protocols and devices	
The need for network models	• To abstract complex physical devices. • To encourage interoperability between different equipment manufacturers. • To standardise subject terminology.
Open systems interconnection (OSI) model	Seven Layer model: • Layer 1 Physical hardware eg signalling, wiring. • Layer 2 Data links eg frames, packets. • Layer 3 Network. • Layer 4 Transport eg streams, segments. • Layer 5 Session eg authentication, encryption. • Layer 6 Presentation. • Layer 7 Application.

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 eg:
	  • network interface cards (NICs)
	  • repeaters
	  • hubs
	  • network layer protocols and devices eg:
	  • 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 eg:
	  • 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.

AO1: 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 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
This performance outcome enhances learners' understanding of circuit and packet switching, LAN Technologies, and WAN technologies.

AO2: 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.

AO3: 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 applications 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

Unit 3 – PO3: Understand 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.

Unit 6 – AO1: Understand potential threats and risks to organisational systems
The network risks described in this assessment outcome are explored further by examining the organisation impact that could occur. Learners should benefit from exploring these concepts from an organisational perspective.

Unit 7 – PO1: Understand the principles of computer forensic investigation
This performance outcome expands the concept of network risks by examining the different uses of hardware and software that can circumvent data, personal or communication security.

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 – AO2: 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 IEEE Institute of Electrical and Electronics Engineers (IEEE) 802 family for LAN, WLAN (Wireless LAN) etc.

Unit 3 – PO5: Undertake end user network testing
This performance outcome asks learners to perform diagnostics on various network physical layer devices, eg network interface cards (NICs).

Useful links and resources

Books

- Dye M, McDonald R and Rufi A, *Network fundamentals*, ISBN 10 1-58713-208-7, Cisco Press, Indianapolis, IN (2008).
- Lammle T, *CompTIA Network+ study guide authorised courseware: exam N10-005*, ISBN 978 1 118 23886-8, John Wiley and Sons, Chichester (2012).
- Steinke S et al, *Network tutorial: a complete introduction to networks*, ISBN 1-57820-302-3, CRC Press, (2003).

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

Title	Developing and maintaining computer networks
Unit number	K/507/6427
Unit assessment type	Centre assessed and externally quality assured
Recommended assessment method	Practical assignment 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.
Guided learning hours	90
Transferable skill(s) contextualised within this unit	Research[4]
Resources required for this unit	A live network environment. Network hardware and software. A range of tools including multimeters, screw drivers, pliers, wire cutters, rubber matting and anti-static wrist bands, lifting and moving equipment. Professional documentation for designing and maintaining networks (may be available from own institution). A range of wiring, conduits, connectors, etc.
Synoptic assessment within this unit	IT: Technical Support linked to Units 1, 2 and 4. IT: User Support linked to Units 1, 2, 4, 5, 6, 7 and 8. Draws on underlying principles of computer applications and data concepts and further develops these concepts with the underlying principles of data communication and the technologies used to build networks. As such many of the building blocks of any networked solution are introduced here. This unit is based on practical activities requiring observance of Health and Safety, linking to computer build and repair activities undertaken in Unit 4. There are many skills, tools and techniques which are common to both the IT technician and the Network specialist; Unit 4 provides clear opportunities for linked learning and assessment through common operational needs. Unit 5 focuses on the correct procedures when installing and maintaining software. Many aspects of network security rely on the selection and use of software solutions to counter internal and external threats. Networks are often at the heart of many businesses and institutions. Unit 6 examines organisational systems security and how a network's design, use and maintenance impacts operational function when faced with internal and external threats. The Industrial project (Unit 8) can provide guidance when defining a networking project's goals, deliverables and scheduling. Extended guidance on synoptic assessment is provided later in this unit documentation.

[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

Communication activities facilitated by computer networks	
Types of personal communication using a computer	(eg) • Blog. • Instagram. • Podcasts. • Email. • Wikis. • Social networks.
Business applications	(eg) • Project management. • Diaries. • Meeting planners. • Spreadsheets. • Databases. • Documents.
E-Business applications	(eg) • Banking. • Retail. • Marketing. • Finance.

Types of network architectures and technology types	
Network architectures	(eg) • Peer-to-peer. • Client/server. • Virtual Local Area Network (VLAN). • Virtual Private Networks (VPN).

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

Wireless local area networks (WLAN) technologies and properties	(eg)
	• Types:
	  • wi-fi 802.11
	  • bluetooth
	• Properties:
	  • 802.11 IEEE standards, eg 802.11b, 802.11g, 802.11n
	  • frequency, eg 2.4 ghz and 5 ghz
	  • speed
	  • distance
	  • interference.

Types of network architectures and technology types	
Wide area network (WAN) technologies and properties	Types eg: • frame relay • Asynchronous Transfer Mode (ATM) • Integrated Services Digital Network (ISDN) • wireless • Very High Bit Rate Digital Subscriber Line (VDSL). • Properties: • speed • distance • transmission media • circuit switch • packet switch.
Wiring standards	(eg) • Coaxial. • Category 5 and 6 Unshielded Twisted Pair (UTP). • Fibre optic.
Network hardware	(eg) • File servers. • Proxy servers. • Connection devices. • Wireless devices.
Connectors	• UTP: • registered jack –RJ connectors eg: • RJ-45 • RJ-11. • Optical fibre connectors eg: • straight tip (ST) • subscriber connector (SC) • mechanical transfer registered jack (MT-RJ) • local connector (LC).
Media converters	(eg) • Single mode fibre to Ethernet. • Fibre to coaxial. • Single mode to multimode.
Cables	(eg) • Serial. • RS 232. • Universal Serial Hub.
Cabling standards	(eg) • 565A. • 565B.

Types of network architectures and technology types	
Cable installation	(eg) • Main distribute frame. • 25 pair. • 110 block. • Broadband over power.
Network connecting devices	(eg) • NIC. • Hub. • Switch. • Basic bridge. • Router.

Network wireless devices	(eg)
	• Wireless access point (WAP).
	• Wireless antennae:
	  • point-to-point (PPP)
	  • point-to-multi-point (PMP).
	• Wireless ethernet bridge.

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

Types of local area networks (LANs) and wide area networks (WANs)	
Local area networks (LAN)	(eg) • Personal area network (PAN). • Enterprise area network (EAN). • Campus area network (CAN).
Wide area network (WAN)	(eg) • Joint academic network (JANET). • Virtual private network (VPN).
Other network types	(eg) • System area network. • Storage area network.

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, multimeters, 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)*
	  • *Workplace (Health, Safety and Welfare) Regulations 1992. Approved Code of Practice and guidance*
	  • *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	

Diagnostic hardware tools	• Tools eg:
	  • multimeter
	  • network multimeter
	  • network cable testers.

Firmware self-diagnostic routines	(eg) • Power on Self-Test (POST). • Network Interface Card (NIC) tests. • Preboot Execution Environment (PXE) boot test.

Simple network management protocol (SNMP)	• Components:
	  • managed device
	  • agent
	  • network management station (NMS).
	• Devices that support SNMP:
	  • routers
	  • switches
	  • servers
	  • workstations
	  • printers.
	• Protocols.
	• Proxy agents.
	• Bilingual network-management systems.

Intrusion detection system (IDS)	• Network intrusion detection system (NIDS). • Host intrusion detection system (HIDS).
Firewall	(eg) • Hardware, software, rules, exceptions, stateful packet inspection (SPI) and application layer.
Diagnostic software tools	(eg) • Control panel (connections, adaptors). • Ping. • Traceroute. • IPconfig/IFconfig. • Netstat. • Nbstat. • Address resolution protocol (ARP).
Steps in trouble shooting	• Identify problem. • Gather information. • Question users. • Look for changes. • Identify possible issues.
Error logs	(eg) • Operating system. • Network service (eg HTTP, FTP) and application.

End user network testing	
Error codes and messages	• Different formats (eg hexadecimal, binary etc) eg generated via hardware, BIOS, operating system, applications and utilities etc.
Documentation	• Recording outcomes and recommendations.

Test plan	• Features to be tested.
	• Features not to be tested.
	• Approach eg testing level, testing types, testing methods.
	• Pass/fail criteria.
	• Test deliverables eg test plan, test cases, test scripts, defect logs, test reports.
	• Test environment:
	  • hardware, software, network
	  • testing tools.
	• Estimate of costs.
	• Schedule ie key milestones.
	• Responsibilities.
	• Test results.
	• Remedial steps taken.
	• Sign off performance.

Maintaining a network system	
Agree a service level agreement (SLA)	(eg) • A description of the services to be provided and for whom. • Roles, responsibilities of team members and contact details. • Availability of the service. • Service standards eg speed of reply to request. • Customer responsibilities. • Legal or other regulations that must be complied with. • Qualitative and quantitative measures to monitor and evaluate service. • Communication methods. • Key performance indicators. • How complaints will be dealt with. • How the agreement will be reviewed and updated.
Complete network documentation	• Records of tests. • Records of installations and upgrades. • Records of issues. • Records of details of resolution of issues.
Carry out preventive maintenance	• Test network for weaknesses eg reduced speeds, loss of connections. • Installing upgrades and new hardware or software. • Installing or upgrading security software. • Monitoring traffic and bottlenecks.

Performance outcomes

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

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

Grading criteria

Performance outcomes	Pass	Merit	Distinction
	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:**
PO1: Identify communication activities facilitated by computer networks	**P1** Describe **nine** activities which are supported by networks.		
PO2: Identify the different types of network architectures and technology types	**P2** Describe **four** architectures.	**M1** Develop a network architecture for a defined user need.	**D1** Justify the choice of network architecture.
	P3 Identify the network components for a defined user need.	**M2** Explain the choice of components.	
PO3: Understand the different types of local area networks (LANs) and wide area networks (WANs)	**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.		

Performance outcomes	Pass	Merit	Distinction
	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:**
PO4: Design and build a network from a specification	**P6** Produce an outline planning document for defined user need.	**M3** Produce diagrammatic representations of the network.	
	P7 Identify the components and the correct tools required to build the network defined.		
	P8 Build the network defined.		
	P9 Follow relevant health and safety regulations when building the network.		
PO5: Undertake end user network testing	**P10** Describe five testing techniques.	**M4** Justify the importance of network benchmarking in system testing.	
	P11 Identify at least **three** network faults on a selected system.		
	P12 Record fault information and create a test plan, identifying the appropriate tools and components required to carry out tests.	**M5** Justify the testing techniques to be used.	
	P13 Carry out tests meeting all health and safety requirements and record the results.	**M6** Analyse the test results.	**D2** Evaluate the testing process.

Performance outcomes	Pass	Merit	Distinction
	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:**
PO6: Maintain a network system	**P14** Provide evidence of following the requirements of an SLA.	**M7** Record and interpret information from complete network documentation.	**D3** Demonstrate preventive maintenance activities in meeting all requirements of the SLA.

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: Demonstrate 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 that are essential aspects of any network architecture and should support the learner in meeting this criterion.

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.

P6: Produce an outline planning document for defined user need

Unit 6 – AO1: Understand potential threats and risks to organisational systems
Unit 6 – AO2: Understand how to secure organisational systems
Unit 6 – AO3: Understand how to protect organisational systems and meet legal and ethical obligations

Unit 6 – AO4: Review and improve a disaster recovery plan
Designing a network requires an appreciation of the goals, requirements and constraints of the organisation. Unit 6 should provide the learner with an understanding of the threats that face an organisation (particularly those reliant on networking), how to ensure operational safety and the legal issues that act as external factors shaping the overall design and implementation.

Unit 8 – PO2: Plan a project with others to meet a specified outcome
Creating planning documents, particularly in terms of setting goals and meeting business requirements is at the heart of this performance outcome for the Industrial project. Many links abound here, particularly when considering constraints, regulatory and legislative requirements and minimum performance requirements.

P7: Identify the components and the correct tools required to build the network defined

Unit 4 – PO1: Build a computer system with hardware and software to meet specific requirements
Designing a network involves the use of special tools. This performance outcome should provide the learner with knowledge of the tools most pertinent to this task, eg cable testers, wire cutters etc. This unit acts as both introduction and reinforcement of their correct (and safe) use when working with network components.

Unit 6 – AO1: Understand potential threats and risks to organisational systems

Unit 6 – AO2: Understand how to secure organisational systems
Unit 6 engages learners in good practices by focusing on internal and external threats that they need to counter when identifying the correct components required to build the network. In addition this unit also focuses on physical (eg cable shielding) and logical (eg encryption, VPNs, hardening, authentication etc) security that can influence the network design by necessitating the use of certain software, hardware or specialist tools.

Unit 7 – PO1: Understand the principles of computer forensic investigation
This unit focuses on the risks associated with certain hardware and software, especially in terms of unauthorised usage. Learners could consider these risks when identifying and selecting the correct components required to build the defined network.

P8: Build the network defined
P9: Follow relevant health and safety regulations when building the network

Unit 4 – PO1: Build a computer system with hardware and software to meet specific requirements
This performance outcome covers a range of system support tools that a typical IT technician may use. Inevitably there is a certain degree of cross-over with many tools (eg cable testers, wire cutters etc) that are also critical for building networked solutions; this unit acts as both introduction and reinforcement of their correct use.

Health and safety requirements also apply to building computer systems and the safe practices and legislation that should be observed are reflected in this unit's first performance outcome. By connecting a 'safety first' approach across these units, the safety of both learners and equipment should be assured. In addition learners will have greater industry awareness of the standards expected when they successfully complete the programme and embark on their new IT career.

P10: Describe five testing techniques

Unit 1 – AO2: Understand 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 BIOS' test functionality, eg checking an integrated LAN/NIC proves to be a viable technique.

Unit 1 – AO3: Understand 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: Perform software installation and implementation
Unit 5 – PO4: Perform software and firmware updates
Unit 5 – PO5: Perform software maintenance to improve system performance
All three of these Unit 5 performance outcomes contribute to a learner's understanding of available testing techniques as they discuss firmware (eg BIOS), patches and updates, drivers, operating system, benchmarking and configuration settings.

Useful links and resources

Journals

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

Books

- Dye M, McDonald R and Rufi A, *Network fundamentals*, ISBN 10 1-58713-208-7, Cisco Press, Indianapolis, IN, 2008.
- Lammle T, CompTIA *Network+ study guide authorised courseware: exam N10-005*, ISBN 978 1 118 23886-8, John Wiley and Sons, Chichester, 2012.
- Steinke S et al, *Network tutorial: a complete introduction to networks*, ISBN 1-57820-302-3, CRC Press, (2003).

Standards

- *IEEE standard for software and system test, IEEE SA 829-2008*: standards.ieee.org/findstds/standard/829-2008.html

12.4 Unit 4: Supporting end users

Title	Supporting end users
Unit number	M/507/6428
Unit assessment type	Centre assessed and externally quality assured
Recommended assessment method	Practical assignment 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.
Guided learning hours	90
Transferable skill(s) contextualised within this unit	Problem-solving [5]
Resources required for this unit	Learners will need access to helpdesk and remote connection software or the opportunity to work as an IT technician on a helpdesk to provide advice and guidance. Support ticket services are available as commercial or open source packages eg Spiceworks, OS Ticket or commercial alternatives. Learners should have experience of communicating with users using a range of techniques, eg remote connections, face-to-face, phone conversations, email etc. Where this might contravene institutional policy Local Area Networks (LANs) or virtual machines could be used. Learners will also need access to practical resources, eg faulty computers and suitable tools and technologies, eg multimeters, cable testers, diagnostic software, remote access software, as listed in the unit content, to troubleshoot problems.

[5] Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.

Synoptic assessment within this unit	IT: Technical Support linked to Units 1 and 3. IT: User Support linked to Units 1, 3, 5, 6 and 8. Draws on experience and knowledge of different types of hardware and software; particularly systems software (operating systems and utilities) as discussed in Unit 1. To provide effective advice and guidance on networks, it is clearly necessary for technical staff to have experience in building and maintaining them as developed in Unit 3. Unit 5 offers content linked to testing when planning software installations and upgrades. Many of these various diagnostic and monitoring tools are also used to diagnose hardware and software faults. IT support staff will often be required to provide advice and guidance on physically securing rooms and buildings that contain technology, as much as having to justify why actions should be taken (legally and ethically). In addition, technical staff should have a good understanding of disaster recovery. These topics are covered in Unit 6. In addition to honing learners' communication skills, the Industrial project (Unit 8) explores planning a solution to a set problem using an organised methodology. Extended guidance on synoptic assessment is provided later in this unit documentation.

Aim and purpose

This unit will equip learners with the knowledge and skills to support end users by resolving a range of technical issues. In doing so the learner will research faults, find and evaluate solutions and communicate effectively with the end user.

Unit introduction

Developments in technology have created a demand for end user support personnel who can help individuals and organisations in different ways. This can include on site helpdesk support or remote support and field support.

End users are often under pressure; learners will develop effective communication skills to interact appropriately with customers and provide end user support as well as seeking support from colleagues, responding quickly and efficiently. Learners will cover diagnosis to solve hardware and software problems, making use of a range of tools and techniques, working safely so as not to endanger themselves and others.

On completing this unit, learners will be able to use their technical knowledge to help end users resolve technical problems. In order to do this, learners will develop skills to select relevant and reliable information from a range of sources.

Learners will also update documentation, eg fault logs, knowledge bases routinely and recognise their importance in future fault diagnosis.

This unit provides an opportunity to evidence achievement of the transferable skill of problem-solving.

Unit content

Building a computer system with hardware and software to meet specific requirements	
Computer equipment and components	(eg) • Motherboard. • CPU. • Internal memory. • PSU. • Fan and heatsink. • RAM. • Hard drive. • Cabling.

Peripherals	• Essential peripherals:
	  • mouse
	  • keyboard
	  • monitor.

Software	(eg) • Systems software. • Applications software.
Configure BIOS	(eg) • Setting date and time. • Set password.
Desktop configuration	(eg) • Icon visibility and icon size. • Font type. • Font size. • Colour. • Background. • Start-up options.
Tools	(eg) • Screwdrivers (Phillips, Allen/hex , spade). • Anti-static wristbands. • Rubber matting. • Multimeter. • Wire strippers. • Wire cutters. • Cable straps.

Building a computer system with hardware and software to meet specific requirements	
Health and safety	(eg) • *Health and Safety at Work Act (1974).* • *Health and Safety (Display Screen Equipment) Regulations (1992).* • *Waste Electrical and Electronic Equipment recycling (WEEE) (2006).* • *The Manual Handling Operations Regulations (1992) (as amended).* • *Workplace (Health, Safety and Welfare) Regulations (1992), Approved Code of Practice and guidance.* • *Electricity at work: Safe working practices (HSE).* • *The Electricity at Work Regulations (1989).* • *Code of Practice for In-service Inspection and Testing of Electrical Equipment (4th Edition).*

How to communicate effectively with end users	
Type of end user	(eg) • Novice. • Experienced. • Technical.
Communication methods	(eg) • Email. • Face-to-face. • Telephone. • Remote access. • Instant messaging services.

Communication techniques	(eg)
	• Body language.
	• Face-to-face.
	• Questioning:
	  • direct questioning
	  • open
	  • closed.
	• Written:
	  • remote access
	  • fault logs
	  • solution/knowledge database.

Type of support	• Outsourcing. • SLAs.
Types of advice	(eg) • Recommendations. • Replacement. • Bug fixes. • Installation of patches. • Reset/reboot instructions.

How to communicate effectively with end users	
Situational communication styles	(eg) • Anger management (customer). • Empathy, patience, tolerance. • Assertive. • Aggressive. • Passive aggressive. • Passive.
Effective communication	(eg) • Clear. • Relevant. • Format (verbal, written). • Interpersonal skills. • Checking understanding. • Response time. • Escalation.

Providing end users with advice and guidance	
Types of fault	• Single-stage faults (simple faults), eg common, easily identifiable, quick solution. • Multi-stage faults, eg complex, unknown, non-specific symptoms.
Sources of information	(eg) • Manuals. • Product specification. • Manufacturer's resources/website/knowledge base. • Colleagues with specialist knowledge. • Fault records and trends. • FAQs. • Technical forums.
Validity of information	(eg) • Cross referencing. • Reliable sources. • Problem reproduction. • Up-to-date. • Valid.

Using appropriate tools to troubleshoot end user problems safely	
Organisation	• Policy. • Procedure.
Working practices	• Obtaining permission. • Preparing the work site. • Documentation. • Recoding information, eg product keys, licenses. • Electrical safety and electro static discharge (ESD). • Correct use of tools, eg screwdrivers, multimeters. • Data security. • Health and safety. • Fire safety. • Other, eg lasers, first aid, tiredness.
Troubleshooting techniques	• Problem replication. • Substitution. • Elimination. • Test. • Upgrade, eg BIOS flashing, device drivers. • Reinstall software, eg drivers, applications. • Bug fixes. • Error codes and messages, different formats, eg Hexadecimal, Binary. • Systematic approaches to troubleshooting.

Software tools	• Diagnostic tools:
	  • virus/malware scanners
	  • monitoring programs
	  • memory testing
	  • operating system tools and logs
	  • specific software applications tools and logs
	  • power on self-test (POST).
	• Monitoring tools:
	  • fault logs
	  • event logs
	  • performance monitoring.
	• Remote connection:
	  • ping test
	  • remote connection
	  • instant messaging (IM).

Hardware tools	• Hardware tools, eg screwdriver, pliers, paper clip, ESD kit. • Test equipment, eg multimeters, cable testers, PSU tester, loop back plug. • Test read instruments, eg CPU, Hard Disk, PSU. • Test machine. • Self-test routines, eg power on self-test (POST), self-monitoring, analysis and reporting technology (SMART).

Using appropriate tools to troubleshoot end user problems safely	

Troubleshooting remedies	• Hardware:
	  • repair
	  • replacement
	  • upgrade.
	• Software:
	  • reconfigure
	  • patches
	  • reinstallation
	  • upgrade.

General legislation	(eg) • *Communications Act (2003).* • *Data Protection Act (1998).* • *Computer Misuse Act (1990).*

Testing solutions and analysing results	
Testing	(eg) • Test data. • Self-test. • Diagnostic tools. • System scans. • Fault logs. • Test reports.

Updating documentation	
Documentation	(eg) • Support ticket. • Fault log. • Solution details. • Test report. • Required resources. • Stock levels/ordering. • Waste disposal. • Feed back to the user. • User feedback and signoff. • Recommendations.

Performance outcomes

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

Performance outcome 1:	Build a computer system with hardware and software to meet specific requirements.
Performance outcome 2:	Understand how to communicate effectively with end users.
Performance outcome 3:	Provide end users with advice and guidance.
Performance outcome 4:	Use appropriate tools to troubleshoot end user problems safely.
Performance outcome 5:	Test solutions and analyse results.
Performance outcome 6:	Update documentation.

Grading criteria

Performance outcomes	Pass	Merit	Distinction
	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:**
PO1: Build a computer system with hardware and software to meet specific requirements	**P1** Set up a basic computer, installing all hardware components and essential peripherals, working safely.		
	P2 Install the operating system and **one** software application.		
	P3 Configure **one** setting in the BIOS and **two** desktop settings.		
	P4 Test the computer for functionality.		
PO2: Understand how to communicate effectively with end users	**P5** Communicate support to **three** different end users using written and verbal techniques.	**M1** Identify instances where situational communication skills would be required.	**D1** Evaluate the effectiveness of communication used and highlight where improvements could be made.

Performance outcomes	Pass	Merit	Distinction
	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:**
	P6 Use **four** different communication methods to provide advice and guidance.		
PO3: Provide end users with advice and guidance	**P7** Analyse information provided by **three** different end users and in each case determine technical advice and guidance required.		
	P8 Respond to faults reported.	**M2** Explain how the advice and guidance has been checked for validity.	**D2** Evaluate the effectiveness of support provided.
PO4: Use appropriate tools to troubleshoot end user problems safely	**P9** Solve **three** single-stage software problems safely, following working practices.	**M3** Solve **two** multi-stage software problem safely, following working practices.	**D3** Justify the solutions selected for solving software faults.
	P10 Select and apply appropriate software tools to solve specific problems.		
	P11 Solve **three** single stage hardware problems safely, following working practices.	**M4** Solve **two** multi-stage hardware problems safely, following working practices.	**D4** Justify the solutions selected for solving hardware faults.
	P12 Explore **two** complex hardware **problems**.		
	P13 Plan, select and apply appropriate hardware tools to **solve** specific **problems**.		

Performance outcomes	Pass	Merit	Distinction
	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:**
PO5: Test solutions and analyse results	**P14** Test software and hardware solutions and resolve issues.	**M5** Analyse tests results and apply appropriate remedies.	**D5** Evaluate the importance of thorough testing on hardware and software resolutions.
	P15 Check if the **problem** has been resolved by testing the hardware solutions and review the **problem-solving process**.		
PO6: Update documentation	**P16** Complete support documentation accurately to meet organisational requirements.		

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 P12, P13 and P15, learners will be presented with an opportunity to demonstrate the transferable skill of problem-solving.

Ideally evidence could come from naturally occurring opportunities (especially if the learner has a work placement) or from activities in other units. If this is the case witness statements and the completed logs and documentation produced naturally by the learner could be used to assess competence. Alternatively learners could be provided with a series of scenarios or fault logs to resolve.

For **P1** to **P4** learners will carry out a practical computer build. Learners should self-select the components, tools and safety equipment (rather than the teacher preparing tables set out with 'everything you need'). Photographs, a witness statement or video would provide good evidence, although teachers might ask learners to develop their own checklist of resources and processes that could then be signed off by the assessor.

For **P5** recordings (audio or video) of learners undertaking fault diagnosis and clearly demonstrating them communicating with users could provide evidence. In doing so learners should demonstrate the ability to communicate with the end user in a range of ways.

For **P9**, **P10**, **P11**, **P12** and **P13** the evidence could come from witness statements, diagnostic printouts, recordings or screen grabs. It is important that these faults should be varied and require different tools to solve in order to give the student a range of assessment opportunities. Examples for

resolution could include: using monitoring software to identify operating system errors with services failing to start; using antivirus software to identify and remove viruses; installing patches to fix faults in software; testing a faulty power supply with a multimeter for a computer that does not start; using a cable tester to check an ethernet cable for a machine unable to connect to a network, followed by a ping test; and using POST to identify malfunctioning or poorly connected hardware devices.

For **M4** it important that tutors appreciate the differences between a single-stage solution and a multi-stage solution when designing a range of assessment activities. These faults should not simply be an expansion of those used for the assessment at pass level.

It is possible that evidence could be naturally occurring in other units and tutors should use evidence from other areas where possible.

It is important that tutors note the health and safety aspect of these criteria. Learners should demonstrate established working practices – for instance the use of an electro static discharge (ESD) kit, appropriate clothing, manual handing and health and safety procedures.

For **D5** learners should focus on two perspectives: the importance of testing from a user's viewpoint and how testing in general is important to industry.

For **P16** learners must generate evidence through records of activities completed.

Employer engagement guidance

If learners are in the workplace then the centre could ask the employer whether there are 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 learners have to practice.

Delivery guidance

Delivery of this unit would be most effective if learners can build links between the classroom and organisations that need to provide end user support. This could be the education centre's own technical support department. Learners will also need to have sufficient practical experience in troubleshooting and solving hardware and software problems.

Delivery could be based on the given order of performance outcomes. However, opportunities for learners to gain work experience where available should be taken. Evidence for practical assessments could be collected in the form of logs, notes, test reports, observation records or witness statements.

Video evidence and role plays can be valuable for developing soft skills and practicing techniques for communicating with end users. Learners will need to practice dealing with annoyed and frustrated users.

Performance outcome 1

Learners should build a basic computer system as defined in the unit content. They will install the operating system and an application, carry out configuration and test to ensure that the system is working.

During the development of the skills for this outcome, there is an opportunity to introduce some non-working components to ensure that learners deal with a variety of situations. Some centres might choose to become involved with the *Computers for Africa* campaign to ensure a good supply of components and machines to be used as part of the learning process.

Performance outcome 2

This centres on the learner's ability to communicate appropriately with end users. Learners could, for example, work with the centre's IT support department for a day (or even just a few hours), shadowing the technical support team to explore how effective communication should be undertaken.

Performance outcome 3

Learners will need to establish skills in finding and validating sources of information from beyond their immediate knowledge. Different sources of information can be researched, analysed and evaluated. Deciding on whether something is valid can be difficult, especially when choosing from a plethora of internet sites that may seem genuine. Learners need to be able to recognise what to look out for to assess validity. Tutors may need to guide learners in methods of researching and using various resources, tools and techniques for troubleshooting.

Performance outcome 4

It is important that learners develop skills in approaching problems. They will need to become familiar with the different tools and techniques used to troubleshoot hardware and software problems.

They need to analyse information and justify the methods they select and use to solve specific problems. They may need to be guided to troubleshoot more complicated problems and record their solutions for future reference.

Tutors must ensure that learners observe health and safety procedures, as well as good working practices when working with IT equipment. They should also understand the impact of good and poor practice.

Performance outcome 5

Learners would benefit from gaining a real understanding of testing in many different scenarios, as it is fundamental to the success of any IT activity – whether it's a network installation, computer build, programme or app. The importance of thorough testing should also be stressed and learners should be challenged not only to test, but to justify the level of testing they have undertaken.

There are many case studies of IT projects that have ultimately failed, or where the cost has risen exponentially, because of a lack of testing.

Performance outcome 6

Learners need to use documentation such as logs methodically, as well as checking that solutions are appropriate. Practical troubleshooting exercises should include keeping logs and updating documentation as part of an ongoing routine.

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: Set up a basic computer, installing all hardware components and essential peripherals, working safely

Unit 1 – AO1: Understand the different types of computer
Learners benefit from a firm understanding of computer types and their common applications as it helps them to identify their basic components.

Unit 1 – AO2: Understand the hardware requirements of a computer system
Learners explore the full hardware requirements of a computer system in this assessment outcome and, as such, it is likely to form their core understanding of the functions of each internal component and the essential peripherals that must be connected to ensure it is functioning correctly.

P2: Install the operating system and one software application

Unit 1 – AO3: Understand the software requirements of a computer system
Learners should be able to differentiate the operating system from a software application if they have a rounded understanding of the different types of software that are available. Unit 1's third assessment outcome focuses on the different types of software available, eg operating systems, applications, utilities etc, categorising them and explaining their basic features and functionality.

P3: Configure one setting in the BIOS and two desktop settings

Unit 1 – AO2: Understand the hardware requirements of a computer system
The basic input output system (BIOS) and extensible firmware interface (EFI) are typically introduced in this unit; consequentially the learner should have prior knowledge of their features and functions, including how to use them to configure the basic operation of the computer system to meet specific requirements.

Unit 1 – AO3: Understand the software requirements of a computer system
Learners may encounter desktop configuration (eg font type, size, colour, background etc) while exploring different operating systems (ie Windows, Apple Mac OS X etc), providing many desktop settings that could be selected here.

P5: Communicate support to three different end users using written and verbal techniques

Unit 8 – PO3: Follow a project plan as part of a team to meet a specified project outcome
Related support information to an end user requires mastery of effective communication, both verbal and non-verbal. Learners hone these skills in the Industrial project (Unit 8) and this should aid them in achieving this grading criterion.

P6: Use four different communication methods to provide advice and guidance

Unit 1 – AO3: Understand the software requirements of a computer system
Of the four most common communication methods that the learner may use to provide advice and guidance to the end user, it is likely that they will have already examined three of these as part of this unit's third assessment outcome: email, remote access and instant messaging. All of these are types of utility or application software.

P7: Analyse information provided by three different end users and in each case determine technical advice and guidance required
P8: Respond to faults reported

Unit 8 – PO3: Follow a project plan as part of a team to meet a specified project outcome
Learners should always consider the needs of the target audience which will differ depending on their relative technical ability. Making these judgements shapes the type of advice and guidance that should be offered. Learners hone these skills in the Industrial project (Unit 8) and this should aid them in achieving this grading criterion.

P9: Solve three single stage software problems safely

Unit 6 – AO3: Understand how to protect organisational systems and meet legal and ethical obligations
Many legislative concerns also affect the behaviour and actions of learners when they are planning and reviewing an organisation's systems security. Learners often appreciate the content and impact of legislation more when it is used in different scenarios, encouraging them to remember it and apply it sensibly.

P10: Select and apply appropriate software tools to solve specific problems

Unit 1 – AO3: Understand the software requirements of a computer system
This unit's assessment outcome focuses on the different types of software available, eg operating systems, applications, utilities etc, categorising them and explaining their basic features and functionality. Learners should have gained 'hands-on' experience with many of the utilities that are used to troubleshoot end user problems, providing extra support for achieving this goal.

Unit 5 – PO4: Perform software and firmware updates
A number of the tools used to troubleshoot software and firmware updates can also be used to troubleshoot end user problems safely. Greater exposure to tools and use in other learning contexts should reinforce their use and potential in learners' minds.

P11: Solve three single stage hardware problems safely, following working practices

Unit 6 – AO3: Understand how to protect organisational systems and meet legal and ethical obligations
As with P9, the legislative concerns also affect the behaviour and actions of learners when they are planning and reviewing an organisation's systems security. This is another opportunity to help learners appreciate the content and impact of legislation: it is used in different scenarios, encouraging them to remember it and apply it sensibly.

P12: Explore two complex hardware problems

Unit 1 – AO2: Understand the hardware requirements of a computer system
Learners explore the full hardware requirements of a computer system in this assessment outcome and, as such, it is likely to form their core understanding of the functions of each internal component and the essential peripherals that must be connected to ensure it is functioning correctly.

P13: Plan, select and apply appropriate hardware tools to solve specific problems
P14: Test software and hardware solutions and resolve issues
P15: Check if the problem has been resolved by testing the hardware solutions and review the problem-solving process

Unit 1 – AO2: Understand the hardware requirements of a computer system
Many of the troubleshooting tools that the learner has to demonstrate correctly are introduced in this introductory unit. Learners could have knowledge and experience of these tools, their (often) acronymic names, eg POST (power-on self-test) and their functionality before commencing this unit.

Unit 3 – PO5: Undertake end user network testing
This unit's performance outcome also focuses on various diagnostic and monitoring tools that could be used by the learner to troubleshoot a specific problem safely. Learners should benefit from using similar tools (eg cable testers etc), in different contexts.

Unit 5 – PO4: Perform software and firmware updates
A number of the tools used to troubleshoot software and firmware updates can also be used to troubleshoot end user problems safely. Greater exposure to tools and use in other learning contexts should reinforce their use and potential in learners' minds.

P16: Complete support documentation accurately to meet organisational requirements

Unit 3 – PO5: Undertake end user network testing
This performance outcome focuses on the different forms of documentation that an IT technician is likely to encounter (and complete) in their role. Many of these are also documents that a Networking specialist might use. Using the same documents in different IT scenarios reinforces both their organisational (and sometimes legal) importance and their correct usage.

Unit 5 – PO6: Document and present systems to users
Creating meaningful documentation is a core aspect of performing both hardware and software installations. Learners will learn how to formally document software installations and updates in this unit and may benefit from comparing and contrasting the two processes.

Useful links and resources

Books

- Meyers M, *CompTIA A+ guide to 802: managing and troubleshooting PCs*, 4th edition, ISBN-10 0071795979, ISBN-13 978-0071795975, McGraw-Hill Osborne, (2013).
- Sanchez A, *Technical support essentials: advice to succeed in technical support (beginner to intermediate)*, ISBN-10 1430225475, ISBN-13 978-1430225478, Apress (2010).

Website

- UK Health and Safety Executive: hse.gov.uk

12.5 Unit 5: Installing and maintaining software

Title	Installing and maintaining software
Unit number	M/507/6493
Unit assessment type	Centre assessed and externally quality assured
Recommended assessment method	Practical assignment 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.
Guided learning hours	90
Transferable skill(s) contextualised within this unit	N/A
Resources required for this unit	Learners will require a range of operating systems eg Windows, Linux, Apple Macintosh OS X, applications and utility software and a range of suitable devices on which to install them. Learners will require access to computers or other devices on which they can install and upgrade software and be able to update firmware. Learners will require access to software, manuals, product keys and registration documents in order to 'sign off' their machines. Access to utilities, eg antivirus, registry cleaners, defragmentation tools and benchmarking software, will be required in order to complete maintenance activities.

Synoptic assessment within this unit	IT: User Support linked to Units 1, 4, 6 and 8. Draws on underlying principles of hardware and software as discussed in Unit 1. This unit includes coverage of organisational risks associated with software and hardware misuse. It is also focuses on disaster recovery concepts such as creating backups, an important step in any software installation or update. There are numerous links to the computer build and repair activities undertaken in Unit 4 as many of the same skills, tools and techniques are exercised when installing (and upgrading) software and hardware. Interpersonal skills also come to the fore here when considering how to question effectively and select the most appropriate communication method. Connections can also be made with the processes involved in formally documenting any changes made to computer systems (whether hardware or software based). Unit 6 includes content on disaster recovery and the reasons why backups are made, which links directly to backups made in this unit. The Industrial project (Unit 8) can provide guidance when defining a user support project's goals, deliverables, scheduling and working to a plan. Aspects of personal communication skills and how to clarify stakeholder requirements also features prominently. Extended guidance on synoptic assessment is provided later in this unit documentation.

Aim and purpose

The aim of this unit is to equip learners with the knowledge and skills to successfully install new software or upgrade existing software, when required by users or companies. Learners will also be able to develop skills and knowledge to ascertain user requirements, plan installation or upgrade activities. Subsequently they will undertake routine maintenance and improve system performance. Learners will also be able to complete documentation as part of the handover process.

Unit introduction

All computer systems rely on a combination of hardware and software to work together harmoniously. For these systems to perform at their best, the software needs to be installed correctly and configured to ensure that the system performs efficiently as well as meeting the needs of the user.

This unit gives learners the opportunity to install and upgrade software in a range of situations. The installation and upgrade of software can range from the local application of a single bug fix, or patch, to a single computer in a small company as an IT technician, to the remote upgrade of an operating system across a global company via outsourcing.

The upgrading of software is an ongoing process using patches to reduce errors, vulnerabilities and hardware issues. However, these fixes can often break other parts of the system. Learners must be able to make sound judgements based on the benefits and drawbacks of any planned changes before any action is taken.

Technicians need to keep coherent records to ensure every job is completed properly and the installation or upgrade meets the customer's needs. Records are also essential to keep track of current versions of software and to help identify problems and trends in reported faults.

The handover will often include a user sign-off to confirm the work has been completed, configured and tested to prove it works. Some organisations use these sign-offs to help with internal charging where the user department pays a contractor or support section for the work carried out for them.

Unit content

Reasons for software installation or upgrade	
Reasons	• (eg) • Reduce costs. • Improve productivity. • Improve system stability. • Improve performance. • Improve security. • Fix bugs. • Additional or new features. • New hardware installations. • User requirements.
Risks	• (eg) • Loss of service. • Loss of data. • Incompatibility issues. • System downtime. • Additional costs.
Risk reduction methods	• (eg) • Data backups. • Low risk times for installation. • Test installation.

Planning and preparing for software installation and upgrade	
Customer	• (eg) • Initial contact. • End user as customer. • Other stakeholders (eg management). • Interview. • Existing software. • Existing configuration. • Set expectations. • Working with customers. • Dealing with difficult customers. • Escalation. • Service level agreement (SLA). • Contracts.

Planning and preparing for software installation and upgrade	
Types of software	• Operating systems. • Applications. • Utilities. • Customisation.
Software licensing	• (eg) • Open source. • Freeware. • Shareware. • End user license agreement (EULA).
Installations	• New installation. • Upgrade.

System requirements	• (eg)
	• Recommended specification.
	• Minimum specification.
	• Recommendations for:
	  • hardware
	  • software
	  • network connectivity.

Planning	• (eg) • Single machine. • Multiple machines. • Permission. • Materials. • Timing. • Technical expertise.
Planning tools	• (eg) • Upgrade paths. • Route maps. • Gantt charts.
Resource allocation	• (eg) • Materials. • Workforce. • Computer availability.
Selection of media/ loading facilities	• (eg) • USB device. • CD/DVD. • Network. • Installation packaging. • Disk images.

Planning and preparing for software installation and upgrade	

Additional considerations	• (eg)
	• Obtaining permission.
	• Sustainability.
	• Decommissioning directives eg:
	  • *Waste Electrical and Electronic Equipment (WEEE) directive (2002/96/EC)*
	  • *Restriction of Hazardous Substances (RoHS) directive (2002/95/EC).*

Compatibility	• Hardware. • Software.

Software installation and implementation	
Tools	• Installation media. • Instruction manual. • License/product key. • Registration. • Media.
Devices	• (eg) • PC. • Laptop. • Smartphone. • Tablet.

Operating systems	• (eg)
	• PC eg Windows, iOS, Linux.
	• Versions eg Windows Start, Business, Enterprise, Ultimate, 32 bit, 64 bit.
	• Portable Devices eg iOS, Android:
	  • configuration
	  • synchronisation.
	• Retail and original equipment manufacturer (OEM) products.
	• Upgrade path.
	• Mounting hard drives.
	• Redundant array of inexpensive/independent disks (RAID).
	• Partitioning eg back up, multiple drives.
	• Recovery disks.
	• Disk imaging/cloning.
	• Dual boot configuration.
	• System repair disks.

Drivers	• (eg) • System components eg onboard graphics, sound, network. • Other eg graphic card, sound card. • Peripherals eg printer, scanner, webcam.

Software installation and implementation	
Application software	• (eg) • Antivirus. • Firewall. • Security. • 'Office' productivity suites eg Open Office, Microsoft Office etc. • Specific applications eg computer aided design (CAD), computer aided manufacturing (CAM), web design.
Configuration	• (eg) • System settings, eg language, time zone. • User rights. • Passwords. • Desktop configuration, eg short cuts or links.
Customisation	• (eg) • Default settings. • Menus. • Toolbars.
Data security	• Confidentiality. • Integrity. • Access.

Performing software and firmware updates	
Patches and updates	• (eg) • Automated and scheduled. • Manual checks. • Service packs.
Firmware	• BIOS eg flashing and recovery, dual BIOS. • Firmware in devices eg router.
Backups	• Automation. • User files. • System files. • Registry and configuration files. • System restore point. • Preservation of data. • Disk image.
Troubleshooting	• Power on self test (POST). • Self monitoring analysis and reporting technology (SMART). • Error codes and messages. • Diagnostic and monitoring software tools. • Error testing.

Performing software maintenance to improve system performance	
Maintenance activities	• (eg) • Removal of installation files. • Removal of unwanted files. • Automatic update configuration. • Clean up, eg internet history, cached files. • Registry cleaning. • Antivirus and Spyware scanning. • Defragmentation. • Start-up programs and services settings. • Virtual memory settings.
Improvements	• (eg) • Boot time. • Speed of processing. • System stability. • Security. • Memory usage. • Storage requirements.
Benchmarking	• (eg) • CPU (eg Dhrystone, Whetstone). • RAM. • Graphics card. • Hard disk. • Network card. • Standards, eg British Association of Public-Safety Communications (BAPCo), the Embedded Microprocessor Benchmark Consortium (EEMBC), Coremark.

Documenting and presenting systems to users	
Completion activities	• Customer acceptance. • Product registration. • Product keys. • Manuals. • Media.
Data integrity	• (eg) • System restore point. • Copy of registration data. • Hard drive image.

Performance outcomes

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

Performance outcome 1:	Identify reasons for software installation or upgrade.
Performance outcome 2:	Plan and prepare for software installation and upgrades.
Performance outcome 3:	Perform software installation and implementation.
Performance outcome 4:	Perform software and firmware updates.
Performance outcome 5:	Perform software maintenance to improve system performance.
Performance outcome 6:	Document and present systems to users.

Grading criteria

Performance outcomes	Pass	Merit	Distinction
	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:**
PO1: Identify reasons for software installation or upgrade	**P1** Describe **four** reasons for the installation of new or upgraded software.	**M1** Explain **four** risks associated with the installation of new or upgraded software and suggest how these could be mitigated.	
PO2: Plan and prepare for software installation and upgrades	**P2** Identify customer requirements for an installation and upgrade.	**M2** Analyse existing software, configurations and licenses.	**D1** Demonstrate effective communication with stakeholders at all stages of an installation or upgrade.
	P3 Use tools to plan an installation **and** an upgrade to meet customer requirements.	**M3** Explain the legal implications related to software licences when installing **and** upgrading software.	**D2** Evaluate the risks involved in the installation and upgrade of software and explain how they could be minimised.

Performance outcomes	Pass	Merit	Distinction
	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:**
	P4 Identify the following requirements for installing and upgrading: • the media to be used • materials needed • timing • any permissions needed • decommissioning considerations.	**M4** Prove compatibility to ensure successful completion of installation and upgrade tasks.	
PO3: Perform software installation and implementation	**P5** Prepare for and carry out the software installation as identified in the plan.	**M5** Monitor and adapt the installation plan, responding to a change in customer requirements.	
	P6 Record the activities undertaken when installing and check that: • drivers are up-to-date • configurations have been set correctly • customisation has been set correctly.		
PO4: Perform software and firmware upgrades	**P7** Identify patches and updates needed for a system or device.		
	P8 Prepare for and carry out the software upgrade as identified in the plan.	**M6** Monitor and adapt the installation plan, responding to a change in customer requirements.	

Performance outcomes	Pass	Merit	Distinction
	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:**
	P9 Record the activities undertaken when upgrading and check that: • drivers are up-to-date • configurations have been set correctly • customisation has been set correctly.		
	P10 Design and implement a backup procedure to preserve data, confidentiality integrity and availability during updating.		
	P11 Demonstrate the correct use of **three** troubleshooting tools to check the system.		
PO5: Perform software maintenance to improve system performance	**P12** Plan and perform **six** routine maintenance activities on a computer system to improve performance.	**M7** Demonstrate the effects of routine maintenance on system performance.	**D3** Evaluate performance changes to computer systems after software maintenance by comparing to original performance.
PO6: Document and present systems to users	**P13** Document the installation and upgrade and present the system to customers for sign-off.	**M8** Explain the importance of maintaining data integrity and how this has been achieved.	

Assessment amplification

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

An over-arching assignment can be used to assess the entire unit's content. If this is undertaken tutors will need to arrange for a series of meetings or communications to take place between customers and learners.

The assessment of an installation and upgrade of software should come from a series of substantial practical activities. For instance, installing an operating system, application software, customisation and configuration etc and not just a small update from a regular source eg updating antivirus software.

For **P2** learners will identify the requirements for both an installation and an upgrade for a system, analysing the availability of the software, ensuring that there are sufficient licences to carry out an installation and checking any configuration needs for **M2**. The analysis could be in the format of a recording, a witness statement, or a document such as a check sheet.

For **D1** the learner is required to continue a dialogue with the user through all stages of an installation and when carrying out an upgrade. This could be regular updates on progress or recommendations on improvements to systems and could be evidenced through a witness statement from the assessor.

For **P3** it is important that learners demonstrate an appreciation of the formality of the planning document.

For **M3** Learners need to prove that they have checked the compatibility of the new software with the existing system – for example checking that the other software will not be in conflict and the machine itself has the correct operating system to accommodate the installation. This should be signed off on the plan.

For **P4** the plan should be enhanced with a list of the resources that will be needed to carry out both the installation and upgrade.

For **M4** learners must check that there are no compatibility issues before beginning the practical activity and this should be signed off by the assessor.

For **M5** the tutor will need to communicate changes in customer requirements, such as number of machines, machine specification, required software etc to allow learners to adapt their activities. This could be via email or memo.

The activities in **P8** and **P9** will mirror those in P5 and P6, with tutors expected to communicate changes that will need to be actioned for **M6**. The change should be different to that in M5.

For **P12** learners should perform a series of activities designed to improve the operation of a computer system. For example, removal of installation files, defragmentation of the hard disk drive, or customisation of the start menu. Benchmarking utilities can be used to ascertain some levels of performance increase.

For **P13** learners should create a completion document to record the activities undertaken to finalise the installation as detailed in the content. Learners will then present the system to users as complete for sign-off. This can be achieved through an additional section on the completion document and a witness statement from the assessor.

Employer engagement guidance

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

Delivery guidance

It is recommended that this unit is taught after Unit 1 (Fundamental principles of computing) as it introduces learners to computer systems and types of software that support the installation and maintenance of software.

Although it is suggested that the unit content is delivered in the order of the performance outcomes it is not the only sequence that could be used. There are some elements of units that could be delivered alongside each other eg the installation of software following a successful computer build.

The tutor should remember that the unit content not only focuses on installing and maintaining software, but also their requirements and how they are managed within small and large organisations.

There should be opportunities for learners to work with systems and time spent shadowing technical staff in the centre would be of benefit.

Performance outcome 1

Learners will need to understand the implications of installing or upgrading software and assess not only potential benefits, but potential risks when installing software. This could be achieved through case studies or discussion activities.

Performance outcome 2

Tutors should create appropriate scenarios to allow learners to practice communicating with customers and ascertaining their requirements. Role play activities are particularly good at testing these skills. Subsequent communication is also recommended to allow learners a context in which to practice planning activities and to enable communication throughout the completion of their installation and upgrade plan.

Learners could be provided with opportunities to review licensing agreements, SLAs and contracts in order to understand the legal elements of their software installation plan.

Learners will need to practice creating planning tools eg Gantt charts for the implementation of large scale upgrades and consider how the upgrades will be delivered, eg USB, DVD or imaging etc.

Performance outcomes 3 and 4

Learners will benefit from installing a wide range of different types of operating system and software. They will also benefit from upgrading any applications they have installed and see the differences in the processes.

Documentation should be clear so that other technical staff can understand the activities that have been undertaken.

For troubleshooting, learners need to work with systems that have problems. This could be achieved through learners shadowing IT support personnel and carrying out supervised repairs, working with the centre's own resources. Learners may well also benefit from discussion around issues with their own technologies at home.

Performance outcome 5

Tutors should ensure that the configuration of software is a meaningful exercise. If changes are made for the sake of it, then learners will fail to contextualise the procedure.

Tutors could use disk images of 'extensively used systems' to allow learners to practice installing from the images and then use maintenance tools to tidy up and configure regular updates, optimising the system. Practice in upgrading firmware will also be required.

Performance outcome 6

Documentation to be used could be drawn down from reliable internet sources, or developed from the centre's own documentation practice.

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 four reasons for the installation of new or upgraded software

Unit 6 – AO1: Understand potential threats and risks to organisational systems
The installation and update of software often occurs as a response to an internal or external threat. The first performance outcome in Unit 6 focuses on these threats and the possible organisational impact that can occur if they are not countered and how their risk is assessed. These types of consideration should provide the learner with an additional depth of understanding when tackling this pass criterion.

P2: Identify customer requirements for an installation and upgrade

Unit 1 – AO1: Understand the different types of computer
Learners benefit from a firm understanding of computers and their common applications as it helps them to identify the customer's requirements more accurately.

Unit 1 – AO3: Understand the software requirements of a computer system
Learners should be more capable of identifying customer requirements if they have a rounded understanding of the different types of software that are available. This unit's assessment outcome focuses on the different types of software available, eg operating systems, applications, utilities etc, categorising them and explaining their basic features and functionality.

Unit 4 – PO2: Understand how to communicate effectively with end users
When the customer requirements are being considered it is worth thinking about the communication method being used (eg email, face to face, telephone etc) and the communication techniques being used, especially in terms of achieving effective questioning. These issues also affect the learner's ability to resolve hardware issues, something that this Unit 4 focuses upon.

Unit 8 – PO3: Follow a project plan as part of a team to meet a specified project outcome
The key to identifying customer requirements correctly is the interpersonal and communication skills of the learner. In addition the learner should be able to clarify the customer (and wider stakeholder) requirements before planning any installation or upgrade in order to prevent errors. The Industrial project focuses on honing these critical skills; this type of investigation exercises them very effectively.

P3: Use tools to plan an installation and an upgrade to meet customer requirements

Unit 8 – PO1: Understand the project planning process
Many planning tools exist to support installation and upgrade of software. The Industrial project introduces the concept of project planning software and examines its functionality. It is likely that one of the core tools for project planning, Gantt charts, may be introduced to the learner at this point. They may apply these skills in this context to chart the actions required to meet the customer requirements.

P4: Identify the following requirements for installing and upgrading:

- the media to be used
- materials needed
- timing
- any permissions needed
- decommissioning considerations.

Unit 8 – PO1: Understand the project planning process
Unit 8 – PO2: Plan a project with others to meet a specified outcome
Unit 8 provides the learner with the skills necessary to plan a project effectively (eg setting goals, dealing with stakeholders, setting a schedule, allocating roles etc). Many of the generic project concepts discussed in this unit may be encountered by the learner in a contextualised fashion, eg obtaining permission and the materials needed before committing to a timeline for completion.

P7: Identify patches and updates needed for a system or device

Unit 1 – AO3: Understand the software requirements of a computer system
Learners may benefit from having prior experience with a software inventory, helping them to keep track of installed software and any records pertaining to previous installs of patches and updates, their outcomes and remedial steps taken (in case of failure).

Unit 4 – PO4: Use appropriate tools to troubleshoot end user problems safely
The application of patches and updates is also a typical troubleshooting remedy and is the focus of learners' work in this unit's performance outcome. Learners may benefit from additional troubleshooting of software issues that are related to causing hardware issues.

P10: Design and implement a backup procedure to preserve data, confidentiality integrity and availability during updating

Unit 1 – AO3: Understand the software requirements of a computer system
The learner is introduced to the concept of a backup tool as an example of utility software in this unit's third assessment outcome. This familiarity may help the learner design their backup procedure.

Unit 6 – AO4: Review and improve a disaster recovery plan
Backups are examined in some detail as part of a disaster recovery strategy in this unit. In particular the unit focuses on different types of backup, their frequency, media and storage locations. Learners explore how to design and implement a more inclusive backup procedure and preserve more data with better integrity having benefited from this additional coverage.

P11: Demonstrate the correct use of three troubleshooting tools to check the system

Unit 1 – AO2: Understand the hardware requirements of a computer system
Many of the troubleshooting tools that the learner has to demonstrate correctly are introduced in this introductory unit. Learners could have knowledge and experience of these tools, their (often) acronymic names, eg POST (power-on self-test) and their functionality before commencing this unit.

Unit 4 – PO4: Use appropriate tools to troubleshoot end user problems safely
Many hardware issues are resolved through the use of software troubleshooting tools. In addition, programs, devices and operating systems often report complex (or obscure) error codes and messages that often require referencing before their meaning can be fully understood. The installation and upgrade of software shares many of these issues so greater exposure to this type of problem-solving should benefit the learner.

P12: Plan and perform six routine maintenance activities on a computer system to improve performance

Unit 1 – AO3: Understand the software requirements of a computer system
Many of the maintenance activities that the learner could perform to improve the performance of the computer system are introduced as utility programs in this unit's third assessment outcome. The learner's awareness of utilities available (and their practical use) should assist the satisfactory completion of this grading criterion.

P13: Document the installation and upgrade and present the system to customers for signoff

Unit 4 – PO5: Test solutions and analyse results
Creating meaningful documentation is a core aspect of performing both hardware and software installation. Learners will learn how to formally document hardware updates in this unit and may benefit from comparing and contrasting the two processes.

Useful links and resources

Books

- Andrews J, *A+ guide to hardware: managing and maintaining your PC*, 8th edition, ISBN-10 1133135080, ISBN-13 978-1133135081, Wadsworth Publishing Co Inc (2012).
- Mueller S, *Upgrading and repairing PCs*, 22nd edition, ISBN-10 0789756102, ISBN-13 978-0789756107, QUE (2013).

Operating system manufacturers

- Microsoft: microsoft.com
- Apple: apple.com
- Linux: linux.com

Utility software

- Registry tools: CCleaner
- Disk imaging: Yumi, Clone zilla, DriveImage XML
- Partitioning: Paragon Partition Manager
- Malware protection: Avast, AVG, Spybot
- Open-source software: Open Office, Libre Office

12.6 Unit 6: Organisational systems security

Title	Organisational systems security
Unit number	T/507/6494
Assessment	Externally assessed
Guided learning hours	90
Transferable skill(s) contextualised within this unit	N/A
Resources required for this unit	Sample polices and plans as listed in the syllabus content. Suitable networked computers and the ability to access the internet to create a VPN or a LAN with VPN capable router to simulate a VPN. Learners should also have access to suitable computers or portable devices and backup software and devices, to allow for practical experience in backing up and restoring data. Suitable computers and security software eg antivirus, firewall as per the unit content.
Synoptic assessment within this unit	IT: User Support linked to Units 1, 3, 4, 5, 7 and 8. Draws on underlying principles of information and software as discussed in Unit 1. Networks are often found at the very heart of modern organisations. In Unit 3 learners focus on network activities and applications that can be disrupted by internal and external threats and also provides additional coverage of the network-based tools that can contribute to an organisation's protection. In Unit 5 learners practically install software that will include the consideration of user credentials and how this must be managed to limit access. Unit 6 flips learners' perspective by asking them to consider how they would circumvent organisational systems security using specialist tools and techniques. In Unit 7, learners will be expected to consider the protection and security of any system implemented. Extended guidance on synoptic assessment is provided later in this unit documentation.

Aim and purpose

The aim of this unit is to equip learners with the knowledge to; assess risks to security systems, take measures to ensure that they remain secure and plan for disasters. In addition learners will perform backups, configure the security of a computer system and create security policy documentation to support employees.

Unit introduction

With our ever-growing reliance on technology and online business activities the security of computer systems and infrastructure has become vital to many companies, large and small, across the globe.

Organisations and customers require confidence that their data is secure from a range of threats. Protection of these assets can only be confirmed by people who are aware of how these threats work and know how to reduce the likelihood of the threat occurring.

Any incident, accidental or premeditated, could be disastrous to an organisation and it is vital to its continuing existence that the organisation has a backup policy, plan and procedure in place to deal with any eventuality and that this is followed correctly by all employees.

Security policies and procedures play a constant role in protecting systems and inform employers and employees of their responsibilities. Regardless of the security measures taken, they can affect our rights as individuals, for instance, the use of social media sites or email privacy. The balance between security and freedom raises a number of important ethical issues that learners need to be aware of. These ethical issues need to be managed effectively in a modern organisation.

Unit content

Potential threats and risks to organisational systems	
Information security	Key aspects: • Confidentiality. • Integrity. • Availability.

Internal threats	• Unauthorised access.
	• Accidental damage.
	• Localised disasters, eg fire, water leak.
	• Human error.
	• Technical error.
	• Equipment failure or damage.
	• Theft or loss of data.
	• Accidental disclosure or deletion.
	• Actions of disgruntled employees:
	  • sabotage
	  • intentional disclosure or deletion.

Potential threats and risks to organisational systems	

External threats	• Accidental damage:
	  • natural disasters.
	• Malicious software:
	  • malware
	  • viruses
	  • spyware
	  • adware
	  • rootkits
	  • zombies
	  • botnets
	  • logic bombs.
	• exploits and backdoors
	• Theft of assets or data:
	  • identity theft
	  • eavesdropping
	  • shoulder surfing
	  • dumpster diving
	  • snooping.
	• Spam.
	• Phishing.
	• Hacking.
	• Zero day attacks.
	• Distributed denial of service (DDoS).
	• Malicious damage.
	• Website defacement.
	• Counterfeit goods:
	  • products at risk eg DVD's games, music, peer–to–peer networks
	  • Trading Standards.
	• Industrial espionage.
	• Copyright infringement.

Organisational impact	• Increased costs. • Loss of service. • Loss of business or income. • Loss of property. • Reputation and customers. • Legal liability.

Potential threats and risks to organisational systems	

Risk assessment	• Risk severity:
	  • low
	  • medium
	  • high.
	• Probability:
	  • unlikely
	  • likely
	  • very likely.
	• Loss:
	  • minor
	  • moderate
	  • major.

Securing organisational systems	

Physical security	• Doors.
	• Locks.
	• Three-barrier system.
	• Mantraps.
	• Cable shielding.
	• Signing in/out procedures.
	• Visitor passes.
	• Smart cards.
	• Access to areas.
	• Biometrics, eg:
	  • retinal scan
	  • finger print scan
	  • voice recognition.
	• Employee training.
	• Code of conduct:
	  • a list of expected behaviours which employees sign toconfirm their intended compliance.
	• Computer misuse.
	• Surveillance.

Securing organisational systems	
Software and network security	• Encryption techniques (public and private). • Virtual private networks (VPNs). • Data encryption. • Passwords. • Access levels. • Software updates. • Firewalls. • Antivirus. • Anti-Spyware. • Copyright. • Software licensing. • Open source. • Shareware and freeware. • Commercial software.
Hardening	• Hotfixes. • Patches. • Service packs. • Pack management. • Group policies.
Authentication methods	• One, two and three-factor authentication. • Single sign-on. • Password updating. • Rigour of passwords.

Protecting organisational systems and meeting legal and ethical obligations	
Codes of conduct and contract Clauses	Formal agreements: • 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.
Legislative requirements	This should consist of the key elements of current legislation: • *Data Protection Act (1998).* • *Computer Misuse Act (1990).* • *Copyrights, Designs and Patents Act (1988).* • *Freedom of Information Act (2000).*

Protecting organisational systems and meeting legal and ethical obligations	

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

Recovering from a disaster	
Disaster recovery policy	• Budget. • Availability of resources, eg physical facilities. • Cost vs benefit. • Human constraints, eg people. • Technology constraints. • Management's view of risk. • Data. • Suppliers.
Plan	• Roles and responsibilities. • Incident response. • Plan initiation. • Procedures.
Sites	• Hot. • Warm. • Cold. • Back-up generator.

Recovering from a disaster	

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.

Assessment outcomes

Learners will be able to:

Assessment outcome 1: Understand potential threats and risks to organisational systems	
a	The key aspects of information security.
b	Types of internal and external threats.
c	The impact on organisations of internal or external threats.
d	Levels of risk assessment and proposed actions.

Assessment outcome 2: Understand how to secure organisational systems	
a	Forms of physical security.
b	Forms of software and network security.
c	The effectiveness of different types of system hardening.
d	Authentication methods and techniques.

Assessment outcome 3: Understand how to protect organisational systems and meet legal and ethical obligations	
a	Formal agreements which contribute to codes of conduct and contract clauses.
b	The scope of current legislation which protects organisations and individuals from threats.
c	The ethical factors that affect organisation systems security.

Assessment outcome 4: Review and improve a disaster recovery plan	
a	Elements of a disaster recovery policy and plan.
b	Forms of relocation site (and contributing technologies) which form part of a disaster recovery plan.
c	Types of backups.

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 but, where appropriate, full working should be shown.

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.

AQA will ensure that the full content of the unit is covered equally over the life of the qualification.

Employer engagement guidance

The organisation, its staff and learners will have access to employers and expertise. The organisation itself will have computer/technical staff who will understand the practical activities identified in the assessment outcomes; the organisation will also have its own policies and procedures.

Employers may be able to provide opportunities to visit IT facilities or provide placement or shadowing opportunities for learners or allow learners to risk assess their organisations.

Where possible, tasks set for learners should be realistic and have a strong vocational context.

Delivery guidance

The nature of this unit means that learners can do significant in-centre research to establish the types of security implemented. They would benefit from a discussion with IT staff and, where possible, should visit external organisations and/or employers to look at different configurations of security elements.

Assessment outcome 1

Learners could perform a number of activities – for instance the assessment of risk, review of security policies etc – in conjunction with local companies or even the centre itself. Using external speakers or the centre's own staff can give a real world view of security. Alternatively discussing the centre's own security techniques and procedures to deal with threats could be another starting point for the delivery of the unit.

The centre will have people who are responsible for policies and procedures related to IT security and using their expertise would be of great value in relating the unit content to workplace activities.

Where this is not available, tutors will have to devise suitable sample documents or cases studies for learners to use.

Learners need a sound knowledge of threats to systems in order to understand potential risks. It is recommended that this is taught first. Analysis of case studies, news articles and exploration of how particular threats occur is vital to the broadening of the learner's knowledge in this area. Learners could be encouraged to share examples that they have been subjected to, eg phishing, or topics that they have researched.

Learners will need practice in completing risk assessments and ascertaining the level of risk posed by a range of threats and their impact.

Assessment 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 these work. They should understand that security can be both logical and physical and they 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.

Assessment outcome 3

Learners should have access to, or could carry out research on, 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.

Assessment outcome 4

It is important that learners are provided with guidance on how to create a formal disaster recovery plan. They need to be aware of all the relevant areas that need to be covered and how this might vary between organisations. Learners could work in groups and review sample plans from other organisations. They should be able to draw on their knowledge of the previous performance outcomes to analyse plans and highlight potential weaknesses.

This could be delivered and assessed alongside a formal security review of a company or via a case study. Learners will need practical experience of creating and restoring a range of backups over time.

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.

AO1: Understand potential threats and risks to organisational systems

Unit 1 – AO4: Understand how data is converted to information
Although learners will discover the key aspects of information security in Unit 4, this particular assessment outcome supplements their understanding by examining issues that can contribute to the quality or validity of the information and how data should be managed to ensure that it is kept confidentially, with integrity and therefore is available when needed. More able learners may be capable of making sensible links between the two, eg accuracy and integrity, for example.

Unit 3 – PO1: Identify communication activities facilitated by computer networks
Many of the internal and external threats are discussed in other units, offering the learner more scope for their research. In addition, some units also focus on the activities and applications that can be badly disrupted by these types of threats. Learners should be able to link the threats to the affected activities and the consequential impact they have on organisations.

AO2: Understand how to secure organisational systems

Unit 1 – AO3: Understand the software requirements of a computer system
Authentication methods are likely to be covered as one of the key functions of an operating system. This unit's approach considers aspects such as controlling user access to devices, programs and data – all key elements that should assist the learner in making the link with organisational system security.

Unit 3 – PO2: Identify the different types of network architectures and technology types
The creation of user accounts with associated passwords and access control lists (ACLs) as part of basic network security links neatly with the theme of authentication. Learners are likely to implement basic user authentication as part of basic network security (and usually as part of traditional client/server architecture). As a consequence learners should be able to relate to their practical experiences when explaining these methods and their contribution to organisational system security.

Unit 3 – PO5: Undertake end user network testing
In this unit learners undertake practical network testing and the importance of this activity is reinforced within Unit 6 as part of the strategy for ensuring that steps taken to secure networks are tested in the first instance and retested periodically to ensure that security is maintained.

Unit 5 – PO3: Perform software installation and implementation
Having the correct user credentials and rights is often a key aspect of successfully installing new software on a computer system. Learners will appreciate the differences between different user rights (in terms of administrative access) and how this affects installation. This could be referenced by the learner as an example of linked learning.

Many of the threats (particularly external) 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 spent with these software tools and should use this experience to enhance their descriptions.

Unit 7 – PO2: Plan a computer forensic investigation
This unit offers another perspective on authentication methods by examining the forensic tools required to crack a computer system's passwords. The need for these tools reflects the significance of the authentication process and how vital it is for organisational system security. The learner may choose to reflect on this as part of their coverage.

AO3: Understand how to protect organisational systems and meet legal and ethical obligations

Unit 4 – PO4: Use appropriate tools to troubleshoot end user problems safely
Many legislative concerns also affect the behaviour and actions of learners when they are supporting end users. Learners often appreciate the content and impact of legislation more when it is used in different scenarios, encouraging them to describe the key elements in a richer level of detail.

AO4: Review and improve a disaster recovery plan

Unit 1 – AO3: Understand the software requirements of a computer system
The learner is introduced to the concepts of encryption and a backup tool as an example of utility software in this unit's third assessment outcome. This familiarity may help learners consider the design of backup procedures that contribute to a disaster recovery plan.

Useful links and resources

- Conklin WA et al, *Principles of computer security: CompTIA Security+ and beyond*, 3rd edition, ISBN-10 0071786198, ISBN-13 978-0071786195, McGraw-Hill Osborne (2012).
- Wheeler E, *Security risk management: building an information security risk management program from the ground up*, ISBN-10 1597496154, ISBN-13 978-1597496155, Syngress (2011).

12.7 Unit 7: Computer forensic investigation

Title	Computer forensic investigation
Unit number	R/507/6440
Unit assessment type	Centre assessed and externally quality assured
Recommended assessment method	Practical assignment 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.
Guided learning hours	90
Transferable skill(s) contextualised within this unit	Communication (oral)[6]
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.

[6] Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.

Synoptic assessment within this unit	IT: User Support linked to Units 1, 4, 5, 6 and 8. Draws on experience and knowledge of different types of software, particularly systems software (operating systems and utilities) as discussed in Unit 1. The building, maintenance and troubleshooting of computer systems often requires knowledge of system events in order to identify unusual patterns of activity or particular errors. Combined with the focus on accurate identification of computer system assets and the creation of precise documentation, Unit 4 provides much of the learner's foundation for studying forensic computing concepts and practices. Unit 5 offers content linked to different types of system software and forensically-relevant utilities while planning software installations and upgrades. 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 6. This unit will help provide learners with a grounding in presentation skills and helps to tune learners' communication skills for target audiences, which is vital for demonstrating the outcome of an investigation or project, making it equally important to Unit 8 (Industrial project). Extended guidance on synoptic assessment is provided later in this unit documentation.

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.

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	(eg)
	• 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.

The principles of computer forensic investigation	
Unauthorised hardware	• Modems. • Key loggers. • I/O devices. • USB devices. • FireWire devices. • Bluetooth devices. • eSATA. • Wireless devices.

Risks associated with software	• Breaches of communications and data security:
	  • IP spoofing
	  • password sniffing
	  • scanning
	  • excess privileges
	  • data attacks, eg:
	  • unauthorised copying of data
	  • traffic analysis
	  • covert channels
	  • data diddling
	  • software attacks, eg:
	  • trap door/back door
	  • session hijacking
	  • tunnelling
	  • timing attacks
	  • trojan horses
	  • viruses and worms
	  • salamis
	  • logic bombs.

Understand file systems and data storage	• FAT, eg:
	  • FAT 16
	  • FAT 32 (Virtual FAT or VFAT)
	  • Extended FAT (exFAT).
	• NTFS.
	• File system metadata.
	• Live, deleted, unallocated data and file stack.

Preinstalled OS tools	(eg) • Event viewer. • Firewall.

Planning a computer forensic investigation	
Evidence life cycle	• Collection and identification. • Storage, preservation and transportation. • Presentation of evidence. • Return to owner or court.

Planning a computer forensic investigation

Four steps of computer forensic investigation	• Acquisition:
	  • search and seizure:
	  • voluntary surrender
	  • subpoena
	  • search warrant.
	• Identification:
	  • relevance of evidence:
	  • proves or disproves facts in a case
	  • admissibility of evidence
	  • legal collection of evidence
	  • not modifying evidence after it has been seized
	  • protect the chain of custody
	  • treat each incident as a criminal act
	  • leave no trace, eg ensuring media is not modified or includes trace that it has been accessed
	  • read-only images
	  • software write blocker
	  • hardware write blocker
	  • types of evidence:
	  • real evidence, eg actual physical evidence
	  • documentary evidence, eg log files, database files, incident-specific files, reports (best evidence rule – original documents not copies)
	  • testimonial evidence, eg witness testimony
	  • demonstrative evidence, eg use of visual aids and other illustrations.
	• Computer forensic software tools:
	  • disk tools and capture
	  • disk imaging software
	  • software or hardware write tools
	  • hashing tools
	  • file recovery programs
	  • analysis software, eg to search and evaluate Internet cookies
	  • encryption decoding software
	  • password cracking software
	  • acquisition of website software
	  • network analysis tools
	  • network discover and security auditing
	  • extraction of RAM dumps
	  • mounting forensic logical and physical disks as read-only.
	• Email analysis.
	• File signatures.

Planning a computer forensic investigation	

Four steps of computer forensic investigation continued	• Mac OS tools eg Mac Memory Reader.
	• Mobile devices eg phone analyser.
	• Data analysis.
	• File viewers.
	• Internet analysis.
	• Registry analysis.
	• Application analysis.
	• Presentation of evidence:
	  • audience
	  • chain of custody:
	  • date
	  • step-by-step process of each activity
	  • explanation of activity, ie what it involves
	  • controls to maintain integrity of evidence eg taking photographs
	  • list of procedures used during collection process with justification of actions
	  • precautions taken to preserve state of evidence eg precautions against disk drive damage
	  • controls to prevent accidental changes to the evidence, eg implementing a write blocker.

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

Performance outcomes	Pass	Merit	Distinction
	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:**
PO1: Understand the principles of computer forensic investigation	**P1** Outline **eight** potential risks associated with the **hardware** of a computer system.	**M1** Explain the issues associated with **four** examples of unauthorised hardware.	
	P2 Outline **eight** potential risks associated with the **software** of a computer system.		
	P3 Describe the file systems of a computer system.	**M2** Explain the data storage on a computer system.	

Performance outcomes	Pass	Merit	Distinction
	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:**
	P4 Explain how **two** pre-installed OS tools can contribute to forensic information.		
PO2: Plan a computer forensic investigation	**P5** Create an annotated diagram of the evidence lifecycle.		
	P6 Explain the admissibility of evidence providing **four** examples of good practice.		
	P7 Identify the types of evidence that could be gathered from the forensic investigation.	**M3** Justify the types of evidence selected.	**D1** Explain the precautions that will be taken to preserve the state of each type of evidence selected.
	P8 Select the following tools to analyse the evidence: • software tools • hardware tools.	**M4** Justify the computer forensic tools selected.	**D2** Explain the importance of the chain of custody process.
PO3: Carry out a computer forensic investigation	**P9** 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.		
	P10 Record the results of the forensic investigation.	**M5** Interpret the results of the forensic investigation.	**D3** Complete *Chain of Custody* documentation.
PO4: Present computer forensic evidence	**P11** **Present** the outcome of the computer forensic investigation.	**M5** Interpret the results of the forensic investigation.	

Performance outcomes	Pass	Merit	Distinction
	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:**
	P12 Provide physical evidence from the computer forensic investigation.	**M6** Review the computer forensic investigation process.	

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 the 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
P2: Outline eight potential risks associated with the software of a computer system

Prior learning on the hardware and software of a system and where these are vulnerable will help learners to identify potential vulnerabilities that could have been breached and therefore may provide some initial opportunities for forensic investigation.

Unit 1 – AO2: Understand the hardware requirements of a computer system
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, anti-virus, etc) discussed in this unit. Learners should benefit from the practical time they have with these software tools and use this experience to enhance their descriptions.

Unit 6 – AO1: Understand potential threats and risks to organisational systems
Many of the potential risks the learner needs to describe here are often viewed as internal and external threats, which are discussed in other units. Learners should be able to link some of the threats that organisations commonly face to hardware issues.

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 operating system (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 and use this experience to enrich their coverage.

Unit 4 – PO4: Use appropriate tools to troubleshoot end user problems safely
One of the preinstalled operating system (OS) tools required here (event viewer) is introduced to the learner in this unit as one of the possible diagnostic tools used for troubleshooting hardware installations and problematic computer builds. Although this is a specific use of this type of tool it provides the learner with additional understanding of its functionality and usefulness when contributing to forensic information.

Unit 5 – PO3: Perform software installation and implementation
One of the preinstalled operating system (OS) tools required here (firewall) may be encountered by the user as a type of application software that they need to configure when installing new software, ie unblocking new software's access to the network. Although this is a specific use of this type of tool it provides the learner with additional understanding of its functionality and usefulness when contributing to forensic information.

Unit 5 – PO4: Perform software and firmware updates
One of the preinstalled OS tools required here (event viewer) is introduced to the learner in the troubleshooting software updates content. Although this is a specific use of this type of tool it provides the learner with additional understanding of its functionality and usefulness when contributing to forensic information.

Unit 6 – AO3: Understand how to protect organisational systems and meet legal and ethical obligations
One of the preinstalled operating system (OS) tools required here (firewall) is considered as part of the logical security that an organisation may use to secure its network. This offers the learner an alternative view that they can use to supplement their answer.

P8: Select the following tools to analyse the evidence:
- software tools
- hardware tools.

Unit 1 – AO3: Understand the software requirements of a computer system
Unit 4 – PO4: Use appropriate tools to troubleshoot end user problems safely
Unit 5 – PO4: Perform software and firmware updates
Unit 6 – AO3: Understand how to protect organisational systems and meet legal and ethical obligations
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

- Clarke N, *Computer forensics: a pocket guide*, ISBN 1849280398, ITGP (2010).
- Farmer D and Wietse V, *Forensic discovery*, ISBN-13 978-0201634976, Addison Wesley (2004).
- Vacca JR, *Computer forensics (computer crime scene investigation)*, 2nd edition. Available from: ganbooks.blogspot.co.uk/2012/09/computer-forensics-computer-crime-scene.html

Websites

- scoop.it/t/computer-forensics-will-get-you
- 7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

12.8 Unit 8: Industrial project

Title	Industrial project
Unit number	A/507/6464
Unit assessment type	Centre assessed and externally quality assured
Recommended assessment method	Practical assignment 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.
Guided learning hours	90
Transferable skill(s) contextualised within this unit	Teamwork[7]
Resources required for this unit	Prior learning and technical resources appropriate for the employer/client brief.
Synoptic assessment within this unit	The Industrial project unit allows centres to demonstrate explicit synoptic assessment. Principally it represents the key opportunity for learners 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 many of the units and outcomes delivered on the IT: User Support pathway. It also affords centres with the chance to creatively exercise the teaching and learning links between the different units and can contribute and promote a holistic delivery programme that encourages the application of prior or concurrent learning. In addition it can be used as a vehicle to provide amplification and aggregation for the grading criteria of internally assessed units into a coherent and technically relevant industry-based task with its sector-specific nature encouraging, developing and assessing learners' use of transferable skills in realistic and demanding contexts. Extended guidance on synoptic assessment is provided later in this unit documentation.

Aim and purpose

To enable learners to participate in a technical project that requires them to work as part of a team. This will help to develop their knowledge, skills and understanding with respect to the project planning and implementation process and the importance of working effectively as part of a team. Learners will undertake a project that reflects the pathway they are following within the overall qualification.

[7] Please visit the specification homepage to access the transferable skills standards and associated guidance and recording documentation.

Unit introduction

The success of a project will depend on how efficient the project team are in executing the project goals and objectives during the project management lifecycle. This will be impacted, in part, by how well work roles are matched to individual competencies, how well members work within a group and whether project milestones are prioritised effectively.

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

Teamwork is important because it creates **human synergy**. It amplifies by producing end results that are greater than the sum of the individual contributions.

The unit is a focal end point, providing opportunities for real synergy across the qualification. It is mandatory as it has been requested by industry. Learners will learn about the project life cycle, resources, issues and methodology. They will be able to produce a project specification and plan as a team for an identified project. Roles and responsibilities will be agreed between the team so that project expectations are clearly understood by all interested stakeholders.

Learners will also learn about the importance of good time management and communication skills in order to facilitate a successful project outcome.

This unit will provide the opportunity for synoptic assessment as learners may undertake projects that are linked to one or more units across the qualification spectrum.

Unit content

The project planning process	
Life cycle	• Analysis phase (eg defining goals, feasibility study, preparing project proposal). • Design phase (eg identifying possible solutions, systems). • Implementation phase (eg creating solution, testing, training). • Evaluation phase (eg project review, feedback from client/user).
Project methodologies	(eg) • Prince 2. • Rapid Application Development (RAD). • Waterfall model. • Structured systems analysis and design methodology (SSADM). • Critical path method (CPM). • as required by Client.
Project problems	• Poor communication (eg between project team members, between stakeholders). • External factors (eg change of project team members, change in finance, timescales). • Lack of project management and leadership. • Conflict between members and/or clients. • Poor tracking of project progress. • Adhering to legislative and organisational requirements. • Unrealistic timescales. • Lack of testing. • Poor quality of product.

The project planning process	
Project planning software and its functionality	(eg) • Project Libre. • Microsoft Project. • Freedcamp.
Benefits of project planning software	• (eg) • File sharing. • Speed of response. • Communication. • Equal access to timescales and tasks.

Planning a project with others to meet a specified outcome	
Stakeholders	(eg) • Project sponsor (funds the entire project). • Business experts (define their requirements for the end product/result). • Project manager (controls the project plan). • Project team (builds the project outcome based on accepted roles and responsibilities). • End user (may be the client or the employees of the client).
Stakeholder expectations	• Level and method of communication used to communication with them. • Kept up-to-date with respect to progress. • How will they measure success? • Outcome of project. • Timescales. • Budgets. • Resources.

Defining project goals	• Review context and requirements of project.
	• Identify key attributes of project:
	  • types of products/services to be delivered
	  • critical constraints eg project duration, costs etc
	  • technologies, tools and techniques to be used
	  • quality requirements to be met
	  • benefits to be achieved.
	• How success will be measured.
	• Must be well defined and measurable.

Project deliverables	• Product or service given to a client.
	• Have due dates (deadline for delivery).
	• Deliverables are:
	  • tangible
	  • measurable
	  • specific.
	• For internal and/or external clients, satisfying a milestone as part of the project plan.

Planning a project with others to meet a specified outcome	

Project schedule	• Required activities and tasks.
	• Resources for each task/activity.
	• Length of time to complete each task/activity.
	• Resource constraints.
	• Develop critical path (tasks dependent on other tasks).
	• Develop schedule – calendar schedule of all tasks with:
	  • estimate of time period
	  • resource required for each task
	  • project team member(s) involved
	  • time on each task
	  • begin and end dates of individual task.

Allocating roles and responsibilities	• Identify roles within project team. • Identify tasks/activities to be carried out. • Define roles based on relevant skills, qualities and knowledge.

Following a project plan as part of a team to meet a specified project outcome	
Time management skills	• (eg) • Set clear goals. • Break down personal goals into discreet steps. • Review personal progress towards identified goals. • Prioritising – order of importance/urgency. • Organisation of work schedule. • List making (eg to do list). • Perseverance (eg take a positive attitude). • Avoid procrastination (eg avoid distractions from noise, emails).
Measuring progress against milestones	• Measure quantity of work output. • Determine whether timelines within plan needs to be modified. • Review their progress with others.
Effective communication	• Interpersonal skills (eg verbal communication skills). • Cues in verbal communication (eg body language, tone of voice). • Questioning techniques (eg open/closed probing). • Written communication (eg note taking, reports, emails, letters). • Understanding the audience (eg who are they, what their knowledge base is). • Clarification of requirements. • Verbal and non-verbal techniques.

Following a project plan as part of a team to meet a specified project outcome	
Effective team meetings	• Agenda available prior to meetings. • Start and end promptly. • Check attendees. • Establish and review ground rules. • Assign administrative roles. • Summarise decisions and assign action items. • Debrief, evaluate and plan for improvement. • Distribute meeting minutes promptly.
Giving constructive feedback	• Provide feedback promptly. • Descriptive. • Not judgemental. • Supportive. • Fair and reasonable. • Positive as well as negative (feedback sandwich).
Receiving feedback	• Pay attention. • Do not become defensive. • Do not launch a counterattack. • Avoid flippancy. • Convey understanding. • Indicate a willingness to work together towards a solution/improvement. • Accept praise graciously.

Reviewing collaborative working as part of a project team	
Review process	• Success of project. • Meeting of objectives. • Factors influencing the outcome (eg work process, external changes, interpersonal aspects).

Performance outcomes

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

Performance outcome 1:	Understand the project planning process.
Performance outcome 2:	Plan a project with others to meet a specified outcome.
Performance outcome 3:	Follow a project plan as part of a team to meet a specified project outcome.
Performance outcome 4:	Review collaborative working as part of a project team.

Grading criteria

Performance outcomes	Pass	Merit	Distinction
	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:**
PO1: Understand the project planning process	**P1** Describe the **four** stages of the project life cycle.		
	P2 Compare the characteristics of **three** project methodologies.		
	P3 Identify **six** of the problems that can occur within a project.	**M1** Explain how the problems identified could be overcome.	
	P4 Compare the functionality of **two** examples of project planning software.	**M2** Explain the benefits of using project planning software in managing a project.	
PO2: Plan a project with others to meet a specified outcome	**P5** Identify a minimum of **two** stakeholders for a specified project.	**M3** Explain the expectations of the stakeholders identified for a specified project.	
	P6 Create a project plan for a specified project.	**M4** Describe in detail **three or more** goals required to complete a specified project.	**D1** Discuss the project deliverables required to meet the goals for a specified project.
	P7 Check the plan with stakeholders to confirm accuracy.		
	P8 Outline the project schedule for a specified project setting clear timelines and milestones.		
	P9 Allocate the roles and responsibilities required for a specified project.		

Performance outcomes	Pass	Merit	Distinction
	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:**
PO3: Follow a project plan as part of a team to meet a specified project outcome	**P10** Effectively plan and manage own time as part of a project team.		
	P11 Carry out agreed roles and responsibilities, negotiating and resolving any conflicts or shortcomings during the project.	**M5** Measure progress against identified milestones.	**D2** Justify any changes to resource and/or milestones.
	P12 Participate in team meetings to discuss project progress.	**M6** Communicate effectively through verbal and non-verbal methods with project team members.	**D3** Explain the importance of effective non-verbal communication.
	P13 Consider feedback received from project team members and make adjustments as appropriate.		
PO4: Review collaborative working as part of a project team	**P14** Reflect on the effectiveness of collaborative working for a specified project.	**M7** Suggest a range of improvements to support collaborative working for future projects.	
	P15 Evaluate your personal contribution to the project.		

Assessment amplification

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

In completing this unit, the process of teamworking will be continually developed and reflected upon.

This unit is best assessed through a single project and would benefit from employer involvement.

Minutes of meetings, development logs, emails, videos or recordings of discussions, written documentation, diagrams and charts, PowerPoint slides as well as the outcome of the project could provide evidence for this unit.

Note: There will be an opportunity to bring in learning from all other units studied and learners should be encouraged to draw on their experience as well as what they have learned.

To address this particular learning outcome, learners must be provided with a scenario that has a specified project outcome. They will be expected to work in teams to produce the project plan, but the individual learner evidence must show how the learner met the assessment criteria for themselves.

For **D3** learners must demonstrate an understanding of non-verbal communication and the problems that inexplicit written communication can cause.

Employer engagement guidance

If learners are in the workplace then the centre could ask the employer whether there are 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 could effectively be used alongside other practical units, which allows learners to work in a team environment.

Performance outcome 1

It is important that learners understand the project planning process and that it is about collaborative working from the outset. Learners need to understand that when working as a team on any project, they have the opportunity to make suggestions, volunteer for specific tasks/activities etc.

Through a class discussion, learners could be given an overview of the project life cycle with emphasis on how they could contribute as a team member. Learners should also have an awareness of the different project methodologies and that different organisations/situations may use different ones.

Problems do occur when working on projects. Therefore it is important that learners have the opportunity to discuss the various issues/problems that could occur, the effect these could have on the project and how they can be overcome (if at all).

Learners could be given project scenarios and in small groups give presentations explaining the problems that may arise, whether they can be overcome and how.

It is also useful at this stage for learners to be introduced to project planning software such as Project Libre and Microsoft Project.

Performance outcome 2

Learners need to understand who the stakeholders are within a project and the fact that the project team is also classified as a stakeholder. Learners could be asked to research different stakeholder types and through a group discussion explain what they believe the individual stakeholder expectations to be. Learners could be given a scenario where they interview different people taking on the roles of various stakeholders in order to establish their expectations.

Part of the project planning process requires discussions with and between stakeholders. Learners could work in small groups or a larger group and discuss the requirements for a specific project. Based on the information they are provided with, they could identify the stakeholders, their expectations, the project goals and deliverables and the project schedule. The groups could give presentations of their plans to the other groups.

Allocating roles and responsibilities is never an easy task when working on projects; learners should be made aware on what basis choices may be made eg experience, knowledge, skills etc. They also need to be aware that they could nominate people for different roles as long as they can justify their choices. Learners could be given different project scenarios to consider (eg setting up a new network) and then: a) identify the roles and responsibilities that would be required in a project team, and b) agree who would carry out the different roles.

Performance outcome 3

In order to carry out their own individual roles and responsibilities effectively, whether working in isolation or as part of a team, it is important that learners develop their time management skills. They could consider the roles and responsibilities that they have been allocated based on the previous scenarios and consider how they will address their time management. They need to be aware of the importance of documenting their time management plans where timescales are involved eg prioritising tasks.

Measuring progress against milestones is important for individual team members as well as the team as a whole. They need to have an understanding of how they measure progress and what they measure it against. In their groups they could discuss how they would measure the team's progress for the project scenario as well as how the individual team members would check their personal progress.

Communication can make or break many a project and it is important that learners understand what effect poor and good communication could have on their project. They could be asked to work in small groups in order to come up with examples of poor communication and its effects on the project outcome. They could also identify examples of good communication and how it can overcome problems/issues as well as other positive effects on the project outcome.

Team meetings also play a big part in projects: they are used to review progress, discuss issues and problems etc. Learners should be taught how to plan, participate in and record team meetings. They could work as large or small project groups and practice planning team meetings, taking an active part in discussions and formally documenting outcomes.

Providing and receiving constructive feedback can be a challenge for many people. Learners need to understand that, especially when working on projects, they may have to provide feedback – for instance telling another team member that they are delaying the project because they have not finished a task, or telling someone that the results of their particular task are not satisfactory. It can also be difficult to give positive feedback without sounding patronising. Learners have to consider their reactions to positive and negative feedback. They should be provided with guidance on how they can provide constructive feedback as well as receive constructive feedback in a positive way. They could practice giving and receiving feedback in pairs based on fictitious scenarios. They could then be provided with feedback on how well they provided and/or received the feedback.

It is suggested that learners are provided with a mini project to work on as a team so that they can apply the knowledge, skills and understanding that they have learnt.

Performance outcome 4

Learners need to understand that when reviewing the success of the project, they should also consider how well the team worked together and how things could be improved for future projects. They need to consider how well the team met the project outcome, and whether there were internal and/or external factors that influenced that outcome. Could these factors have been handled more effectively by the team, or did they play a part in the problems that the team had? Did everyone play their part as agreed, or was the team let down by others?

As a group, they could discuss the outcome of their mini project from PO3 and use their newfound skills in providing and receiving constructive feedback on how they carried out their individual roles and responsibilities, and how they felt other team members performed.

They could be asked to consider how they could improve their collaborative working as a team for future projects to prevent similar issues arising.

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.

IT: Programming project #1

A local baker has successfully run a high street pastry and cake shop for a number of years. Due to the boom in artisan bakery, business is rising and they are considering expanding into a number of premises and offering their goods online through an e-commerce solution. A delivery service is also being considered with drivers being linked to the shops via specialist applications running on mobile devices, providing them with customer and order delivery information in real-time.

As part of this expansion, the baker will understandably require new computer systems which are securely connected to process customer sales, online orders and their accounts with suitable external links to permit internet access (world wide web and email etc). Effective management of the business will also rely on using the internet to survey competitors and promote the business, eg through a dynamic and interactive website which customers can use to check latest offers, make orders and book deliveries.

Administration users will need suitable client PCs, secured from threats, which will provide the typical office-style business software suites, sector-specific applications and safe access to the internet.

One of the key attractions of the business is being able to track customer buying trends and offer loyalty discounts to promote products which need a sales boost. This typically involves calculation of average sales orders, probabilities of different types of discounts (eg free delivery, vouchers etc) affecting shop sales.

Having worked successfully with your company before, the baker has asked you to draw up suitable plans for the installation of the hardware and bespoke software needed and the network infrastructure that is also required to meet their needs. Full documentation is required before a presentational handover occurs and it is assumed that further consultation may also be needed to refine details and answer further queries should they arise.

Although management and employees of this company have basic IT skills, documentation should be as inclusive as possible and use jargon sparingly whilst explaining technical details clearly and concisely.

You are part of the team assigned to complete this task and must complete it within the desired timeframe. How you manage your time, resources and priorities to finish this project is your decision.

IT: Programming project #1

Unit 1 – Fundamental principles of computing

This unit provides underpinning knowledge that supports learners' investigation into the client's needs, principally the hardware and software that is required to fulfil the project. For hardware this would include not only the computer systems required but the communication methods and external hardware (input, output and external backing storage devices).

In addition the learner will benefit from an appreciation of data, information and the data-processing cycle as these will assist their planning and problem-solving when considering how the client will use the computer systems to support their business needs (eg data entry, processing, storage and required outputs).

Key synoptic links:

Unit 1 – AO1: Identify the different types of computer
Unit 1 – AO2: Understand and evaluate the hardware requirements of a computer system
Unit 1 – AO3: Understand the software requirements of a computer system
Unit 1 – AO4: Understand how data is converted to information
Unit 1 – AO5: Demonstrate how computers process user requirements

Unit 2 – Computer programming

This unit supports learners to complete this project by introducing them to the different aspects of computer programming that may be used to meet the client's needs. Principally this will involve the use of different design tools, procedural algorithms, user interfaces and appropriate programming languages to collect customer, product and order data, process it in a secure and efficient manner and produce meaningful information.

Key synoptic links:

Unit 2 – AO1: Understand the different types of computer programming languages and their common uses
Unit 2 – AO2: Analyse the tools and techniques for planning, design and development
Unit 2 – AO3: Evaluate the key features and techniques used in computer programming
Unit 2 – AO4: Demonstrate the principles of good program practice and user interface design

Unit 3 – Website technologies

A key aspect of this project will involve the creation (or tailoring) of an e-commerce system designed to sell the baker's products through an online shopping experience. Many of the skills and techniques learners develop throughout the qualification contribute to this key project component, including an appreciation of the website technologies required and practical skills in markup languages, relational databases, and client-side and server-side scripting languages. Learners may also benefit from examining website vulnerabilities in order to counter them and ensure that their solution is robust and secure for customer use.

Key synoptic links:

Unit 3 – PO1: Understand the key features of website technologies
Unit 3 – PO2: Demonstrate the key features and functions of a markup language
Unit 3 – PO3: Demonstrate the key features of a style-sheet language
Unit 3 – PO4: Demonstrate the key features and functions of a client-side scripting language
Unit 3 – PO5: Demonstrate the key features and functions of a server-side scripting language
Unit 3 – PO6: Recognise vulnerabilities and counter threats to website technologies

IT: Programming project #1

Unit 4 – Mobile applications programming

The client's requirement for a specialist application that runs on a mobile device neatly incorporates the learner's understanding of programming mobile applications. It is likely that the majority of the learner's skills in this discipline will be exercised by this task including key features and functions, the correct design tools and techniques, practical use of mobile development tools and the ability to create and deploy the solution to the correct platform.

Key synoptic links:

Unit 4 – PO1: Understand the key features of mobile application development
Unit 4 – PO2: Apply the key features and functions of mobile application programming languages
Unit 4 – PO3: Demonstrate the ability to design mobile applications
Unit 4 – PO4: Demonstrate the proficient use of mobile development tools
Unit 4 – PO5: Create and deploy a working mobile application using cross-platform development

Unit 5 – Mathematics for computing

Maths features prominently throughout the project, from the basic arithmetic needed to calculate project costs and timeframes to the statistical analysis required to determine customer buying trends and calculate appropriate discounts.

Learners could also benefit from skills developed when working with different number systems as many hardware error codes are displayed in hexadecimal format. Programming logic invariably relies on Boolean logic when creating conditions for controlling selections and iterations. Techniques used to gather and interpret data should also provide vital support for learners when testing their project solution and supporting the success (or otherwise) of its outcome.

Key synoptic links:

Unit 5 – AO1: Understand and manipulate data in common number systems
Unit 5 – AO2: Understand and apply the foundations of computer logic
Unit 5 – AO3: Understand and interpret information using sets, sequences, series, probability and recursion
Unit 5 – AO4: Apply arithmetic expressions to abstract real world ideas
Unit 5 – AO5: Apply matrix methods to solve problems

Unit 6 – Event driven programming

Building software for the website, shop or driver's mobile application could leverage elements of event driven programming. If this is the case the learner should be able to demonstrate many of the concepts and techniques they have assimilated in this unit to solve the problem appropriately.

Key synoptic links:

Unit 6 – PO1: Understand the key features of event driven programming languages
Unit 6 – PO2: Demonstrate the use of event driven language features and functions
Unit 6 – PO3: Demonstrate the ability to design event driven applications
Unit 6 – PO4: Implement event driven applications to a professional standard

IT: Programming project #1

Unit 7 – Object oriented programming
Building software for the website, shop or driver's mobile application could leverage elements of object oriented programming. If this is the case the learner should be able to demonstrate many of the concepts and techniques they have assimilated in this unit to solve the problem appropriately.

Key synoptic links:

Unit 7 – PO1: Understand object oriented programming
Unit 7 – PO2: Design software solutions using an object oriented approach
Unit 7 – PO3: Implement object oriented applications to a professional standard
Unit 7 – PO4: Understand how to test and maintain programs
Unit 7 – PO5: Understand how to produce documentation

IT: Programming project #2

A local bowling centre is refitting its site as a result of progressive new ownership.

They will require new computer systems which are securely connected as a network to process customer bookings, provide computerised scoring and automated features on each lane, with suitable external links to permit internet access (world wide web and email etc) and data connectivity to other sites in the business to promote centre-based competitions and league tables.

Effective management of the business will also rely on using the internet to survey competitors and promote the business, eg through a dynamic and interactive website which customers can use to check latest offers, book sessions and track their playing statistics etc.

Administration users will also need suitable client PCs, secured from threats, which will provide the typical office-style business software suites, sector-specific applications and safe access to the internet. Game Marshals, who patrol the lanes, will need constant mobile communication and the ability to check game scores, reset lanes and clocks in real-time.

One of the key attractions of the business is the tracking software being used to monitor individual customer and team performances when bowling. This typically involves calculation of average performance levels, winning probabilities and playing trends.

Having worked successfully with your company before, the new owners have asked you to draw up suitable plans for the installation of the hardware and software needed and the network infrastructure that is also required to meet their needs. Full documentation is required before a presentational handover occurs and it is assumed that further consultation may also be needed to refine details and answer further queries should they arise.

Although management and employees of this company have basic IT skills, documentation should be as inclusive as possible and use jargon sparingly whilst explaining technical details clearly and concisely.

You are part of the team assigned to complete this task and must complete it within the desired timeframe. How you manage your time, resources and priorities to finish this project is your decision.

IT: Programming project #2

Unit 1 – Fundamental principles of computing

This unit provides underpinning knowledge that supports learners' investigation into the client's needs, principally the hardware and software that is required to fulfil the project. For hardware this would include not only the computer systems required but the communication methods and external hardware (input, output and external backing storage devices).

In addition the learner will benefit from an appreciation of data, information and the data-processing cycle as these will assist their planning and problem-solving when considering how the client will use the computer systems to support their business needs (eg data entry, processing, storage and required outputs).

Key synoptic links:

Unit 1 – AO1: Identify the different types of computer
Unit 1 – AO2: Understand and evaluate the hardware requirements of a computer system
Unit 1 – AO3: Understand the software requirements of a computer system
Unit 1 – AO4: Understand how data is converted to information
Unit 1 – AO5: Demonstrate how computers process user requirements

Unit 2 – Computer programming

This unit supports learners to complete this project by introducing them to the different aspects of computer programming that may be used to meet the client's needs. Principally this will involve the use of different design tools, procedural algorithms, user interfaces and appropriate programming languages to collect customer and game data, process it in a secure and efficient manner and produce meaningful information.

Key synoptic links:

Unit 2 – AO1: Understand the different types of computer programming languages and their common uses
Unit 2 – AO2: Analyse the tools and techniques for planning, design and development
Unit 2 – AO3: Evaluate the key features and techniques used in computer programming
Unit 2 – AO4: Demonstrate the principles of good program practice and user interface design

Unit 3 – Website technologies

A key aspect of this project will involve the creation (or tailoring) of an e-commerce system designed to book bowling sessions and lanes through an online service. Many of the skills and techniques learners develop throughout this qualification contribute to the creation of this key project component, including an appreciation of the website technologies required and practical skills in markup languages, relational databases, and client-side and server-side scripting languages. Learners may also benefit from examining website vulnerabilities in order to counter them and ensure that their solution is robust and secure for customer use.

Key synoptic links:

Unit 3 – PO1: Understand the key features of website technologies
Unit 3 – PO2: Demonstrate the key features and functions of a markup language
Unit 3 – PO3: Demonstrate the key features of a style-sheet language
Unit 3 – PO4: Demonstrate the key features and functions of a client-side scripting language
Unit 3 – PO5: Demonstrate the key features and functions of a server-side scripting language
Unit 3 – PO6: Recognise vulnerabilities and counter threats to website technologies

IT: Programming project #2

Unit 4 – Mobile applications programming

The client's requirement for a specialist application that runs on a mobile device neatly incorporates the learner's understanding of programming mobile applications. It is likely that the majority of the learner's skills in this discipline will be exercised by this task including key features and functions, design tools and techniques, practical use of mobile development tools and the ability to create and deploy the solution to the correct platform.

Key synoptic links:

Unit 4 – PO1: Understand the key features of mobile application development
Unit 4 – PO2: Apply the key features and functions of mobile application programming languages
Unit 4 – PO3: Demonstrate the ability to design mobile applications
Unit 4 – PO4: Demonstrate the proficient use of mobile development tools
Unit 4 – PO5: Create and deploy a working mobile application using cross-platform development

Unit 5 – Mathematics for computing

Maths features prominently throughout the project, from the basic arithmetic needed to calculate project costs and timeframes to the statistical analysis required to determine customer booking trends and calculate appropriate discounts.

Learners could also benefit from skills developed when working with different number systems, as many hardware error codes are displayed in hexadecimal format. Programming logic invariably relies on Boolean logic when creating conditions for controlling selections and iterations. Techniques used to gather and interpret data should also provide vital support for learners when testing their project solution and supporting the success (or otherwise) of its outcome.

Key synoptic links:

Unit 5 – AO1: Understand and manipulate data in common number systems
Unit 5 – AO2: Understand and apply the foundations of computer logic
Unit 5 – AO3: Understand and interpret information using sets, sequences, series, probability and recursion
Unit 5 – AO4: Apply arithmetic expressions to abstract real world ideas
Unit 5 – AO5: Apply matrix methods to solve problems

Unit 6 – Event driven programming

Building software for the website, shop or marshalls' mobile application could leverage elements of event driven programming. If this is the case the learner should be able to demonstrate many of the concepts and techniques they have assimilated in this unit to solve the problem appropriately.

Key synoptic links:

Unit 6 – PO1: Understand the key features of event driven programming languages
Unit 6 – PO2: Demonstrate the use of event driven language features and functions
Unit 6 – PO3: Demonstrate the ability to design event driven applications
Unit 6 – PO4: Implement event driven applications to a professional standard

Unit 7 – Object oriented programming

Building software for the website, shop or marshalls' mobile application could leverage elements of object oriented programming. If this is the case the learner should be able to demonstrate many of the concepts and techniques they have assimilated in this unit to solve the problem appropriately.

Key synoptic links:

Unit 7 – PO1: Understand object oriented programming
Unit 7 – PO2: Design software solutions using an object oriented approach
Unit 7 – PO3: Implement object oriented applications to a professional standard
Unit 7 – PO4: Understand how to test and maintain programs
Unit 7 – PO5: Understand how to produce document

Useful links and resources

Resources will very much depend on what the scenarios are that the centre wishes to use as this unit could be used for any of the pathways.

Book

- Major I, Greenwood A and Goodman M, *The definitive guide to project management*, ISBN-10 0273663976, Financial Times/Prentice Hall (2003).

Websites

- Freedcamp (free project-management software): freedcamp.com
- Project Libre (free project-planning software): projectlibre.org
- Project management lifecycle: mpmm.com/project-management-methodology.php

13 Externally set and marked examinations

13.1 Introduction

The Foundation Technical Level (360 GLH) in IT: Technical Support (TVQ01014) 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: User Support (TVQ01012) qualification unit T/507/6494 (Organisational systems security) 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

Unit title	Fundamental principles of computing
Exam sessions	January and June
Duration	2 hours
Type of exam	Written exam A mixture of multiple choice, short answer and case study type questions.
Number of marks	80
Weighting of unit	25% of IT: Technical Support (TVQ01014) 12.5% of IT: User Support (TVQ01012)

Unit title	Communication technologies
Exam sessions	January and June
Duration	2 hours
Type of exam	Written exam A mixture of multiple choice, short answer and case study type questions.
Number of marks	80
Weighting of unit	25% of IT: Technical Support (TVQ01014) 12.5% of IT: User Support (TVQ01012)

Unit title	Organisational systems security
Exam sessions	January and June
Duration	2 hours
Type of exam	Written exam A mixture of multiple choice, short answer and case study type questions.
Number of marks	80
Weighting of unit	12.5% of IT: User Support (TVQ01012)

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: Technical Support (TVQ01014) qualification units K/507/6427 (Developing and maintaining computer networks) and M/507/6428 (Supporting end users) are internally assessed by the centre.

For the Technical Level (720 GLH) in IT: User Support (TVQ01012) qualification units M/507/6493 (Installing and maintaining software), R/507/6440 (Computer forensic investigation) and A/507/6464 (Industrial project) 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, ie 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: Technical Support (TVQ01014) qualification is graded as P, M, D, D*.

The overall Technical Level in IT: User Support (TVQ01012) 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 1: Points per grade

Grade	Internally/centre assessed unit
Pass	36
Merit	54
Distinction	72

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: Technical Support is 288.

The total possible number of points that can be achieved for the Technical Level (720 GLH) in IT: User Support is 576.

Points for overall qualification grade

Table 2: Foundation Technical Level (360 GLH) in IT: Technical Support (TVQ01014)

Grade	Points boundary
P	144
M	198
D	252
D*	270

Table 3: Technical Level (720 GLH) in IT: User Support (TVQ01012)

Grade	Points boundary
PP	288
MP	360
MM	396
DM	468
DD	504
D*D	522
D*D*	540

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[8]

- 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.

[8] For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills

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 handout, 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[9]

- 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.

[9] For evidence marked with an asterix (*) recording documents are available for centres to use – please see aqa.org.uk/tech-levels/transferable-skills

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[10]

- 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[11]

- 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 evidence[12]

- 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.

Realising potential

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

aqa.org.uk

G02013i