Higher National Unit specification

General information

Unit title: Internet of Things (SCQF level 7)

Unit code: J0HC 34

Superclass:	CC
Publication date:	August 2018
Source:	Scottish Qualifications Authority
Version:	02

Unit purpose

The purpose of this unit is to introduce learners to the Internet of Things (IoT). This unit entails the history of IoT, where the concept has come from, through to modern-day IoT devices and real-world implementations. A deep focus is placed on the different industries that use IoT devices and how collected data can be utilised. A key part of this unit is to introduce learners to the risks associated with various IoT devices, but more importantly, how these risks can be reduced.

This is a **non-specialist** unit that is suitable for learners who have an interest in cyber security, especially computer hardware, networking, ethical hacking and software development. It is also appropriate for learners who are studying courses in Science, Technology, Engineering or Mathematics (STEM). Due to the growing demand for IoT in all industries, this unit allows learners to gather relevant skills that are in high demand in the workplace.

On completion of this unit, learners will be able to identify IoT concepts and will have developed knowledge of devices, implementations, protocols, security concerns and device security vulnerabilities of the IoT. After completion of this unit, learners may progress to further HN units, especially those related to cyber security.

Outcomes

On successful completion of the unit, the learner will be able to:

1 Describe the Internet of Things and its real world implementations.
2 Explain Internet of Things communication protocols and how data can be used.
3 Implement an Internet of Things device to collect meaningful data.
4 Improve the security of an Internet of Things device.

Higher National Unit specification: General information (cont)

Unit title: Internet of Things (SCQF level 7)

Credit points and level

1 Higher National unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7).

Recommended entry to the unit

No previous knowledge or experience is required. However, it would be beneficial if learners had an interest in modern-day computing, cyber security and networking. This may be evidenced by possession of an NPA in Cyber Security and/or computing-related qualifications with a technical focus. Some previous knowledge of networking and data communications is desirable but not essential.

Core Skills

Achievement of this Unit gives automatic certification of the following Core Skills component:

Complete Core Skill	None
Core Skill component	Critical Thinking at SCQF level 5

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of this Unit specification.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

It is suggested that this unit be delivered as part of the HNC Cyber Security. Due to the nature of the IoT and its devices, it is also advisable that this unit is mixed in with other relevant units. For example, learners can use skills that are learned throughout J0HB 34 *Penetration Testing* and apply their practical knowledge on concepts from this unit.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

Higher National Unit Specification: Statement of standards

Unit title: Internet of Things (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Describe the Internet of Things and its real world implementations.

Knowledge and/or skills

- History of the IoT
- Various industries that use the IoT
- Common business models that use the IoT
- Definition of smart city and types of sensors that can be utilised
- Uses for a number of common IoT devices
- Advantages and disadvantages of a number of IoT devices
- Definition of IoT
- Common IoT themes
- Examples of real world implementations

Outcome 2

Explain Internet of Things communication protocols and how data can be used.

Knowledge and/or skills

- Main types of internet communication protocols
- Communication methods of IoT devices across the public internet
- Definition of IP address and why IoT devices require them
- Benefits and caveats of large scale data collection
- Uses of big data in the modern world

Outcome 3

Implement an Internet of Things device to collect meaningful data.

Knowledge and/or skills

- Types of data
- Justification of the selected IoT device
- Installation of the IoT device
- Uses of the chosen IoT device
- Data collection from the IoT device
- Analysis of the collected data

Unit title: Internet of Things (SCQF level 7)

Outcome 4

Improve the security of an Internet of Things device.

Knowledge and/or skills

- Identification of security vulnerabilities of a given IoT device
- Recognition of outdated and vulnerable communication protocols
- Security features to reduce the risk of an attack
- Security testing of an IoT device
- Ways to make an IoT device more secure

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence (Outcomes 1 and 2)
2 Product evidence (Outcomes 3 and 4)

The **knowledge evidence** will relate to Outcomes 1 and 2. It will comprise the knowledge required in these two outcomes. The following knowledge must be demonstrated:

- History of IoT
- Recognition of different industries and business models using the IoT
- Definition of smart cities
- Descriptions and uses for IoT devices
- Descriptions of advantages and disadvantages of IoT devices
- Examples of real world implementations
- Brief explanations of internet communication protocols
- Outline of how IoT devices send data across the public internet
- Brief explanation of IP addresses and why IoT devices require them
- List of benefits and disadvantages of large scale data collection
- Recognition of big data and examples of how it can be used in the modern world

The knowledge evidence may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

The knowledge evidence is required for all knowledge and/or skills statements in Outcomes 1 and 2. It may be sampled when a traditional test is used. When testing is used, it must be under supervised conditions and it must be controlled in terms of location and timing. Access to reference material is not permitted.

The **product evidence** will cover Outcomes 3 and 4. These two outcomes are more suited to practical and hands-on tasks.

Unit title: Internet of Things (SCQF level 7)

Learners are required to choose, install and implement **at least** one IoT device to collect meaningful data. They will then identify vulnerabilities of the chosen IoT device, identify potential cyber-attacks, and improve the device by implementing security features. The product evidence should be recorded in an appropriate format. The evidence for Outcomes 3 and 4 should be produced over a set period of time. This should be open-book and access to materials is permitted. Learners should make good use of referencing and linking to external information. Learners must produce the product evidence independently.

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. Appropriate level descriptors should be used when making judgements about the evidence.

When evidence is produced in loosely controlled conditions, it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

Higher National Unit Support Notes

Unit title: Internet of Things (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1 takes a theory approach to the concept of IoT. It is suggested that the history of the IoT is delivered covering the general creation of the concept, through to more modern-day installations. Information should be covered in relation to the different industries that are using the IoT for a specific reason. For example, it might be that an oil and gas company is using an IoT device to collect well pressure, whilst a local council might use an IoT device to monitor the amount of grit remaining in a street-side grit bin. Educators should provide an overview of smart city and describe how everything could be connected to the IoT cloud/internet. It is suggested that during the delivery of the above materials, a focus should be placed on actual IoT hardware related to the topic and further discussion on the advantages and disadvantages of it should be encouraged.

Outcome 2 takes a theory approach once again. This outcome looks at the data that is collected by an IoT device and how it can be used. This outcome takes a computer science approach as well as a networking view. Time should be spent on covering the main types of IoT communication protocols, such as Transmission Control Protocol (TCP) and/or User Datagram Protocol (UDP). The concept of IPv4 and IPv6 should be described and, more importantly, how the two protocols play the most fundamental part of the internet. The notion of Big Data plays a large part in the IoT and how companies use the data is of high importance. There are countless advantages to large scale IoT data collection, such as being able to draw a baseline of what a ‘normal’ situation would look like. However, if this data contains private information, it would cause an issue if it were to be stolen/lost.

Outcome 3 takes a hands-on approach to learning and this is strongly encouraged. It is up to the discretion of centres; however, it is highly recommended that this approach be taken. Learners should research an IoT device and then physically install one. There has to be reasoning behind why one IoT device was chosen over another. The installed IoT device should be able to collect and send some sort of meaningful data. Then, it would be commonplace for the learner to analyse the data and write a report and statement about it. If a centre is unable to facilitate a physical estate of IoT devices, then it is suggested that this is done virtually.

Lastly, **Outcome 4** builds upon Outcome 3 but focuses on the security of the device. The learner should focus on a range of security vulnerabilities of the IoT device. Then, notes should be made on how to make the device more secure and robust. It is in this outcome that outdated and insecure data communication protocols should be discussed.

Outcomes 3 and 4 are considered to be taught outcomes, whereby learners will apply practical skills, so a focus should be placed on learners working independently.

Due to the nature of IT and cyber security roles, it is recommended that learners get hands-on lab time with IoT devices. If this is not possible, a virtual/simulated environment is also appropriate to use.

Moreover, the general concept of IoT cyber security plays a large part in the whole unit, as opposed to a specific outcome in itself.

Guidance on approaches to delivery of this unit

A suggested distribution of time, across the outcomes, is:

Outcome 1:	10 hours
Outcome 2:	10 hours
Outcome 3:	10 hours
Outcome 4:	10 hours

Summative assessment may be carried out at any time. However, when testing is used it is recommended that this be carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

It is suggested that the centre delivers Outcomes 1 and 2 together. Summative assessment could take place after completion of the first two outcomes. The centre could then move to Outcomes 3 and 4. Outcomes 3 and 4 take a more hands-on approach and a report is more closely related to this type of learning and delivery.

The assessment for the **knowledge evidence** will, most likely, comprise one single assessment and both outcomes will be contained within it. This could be a selected response test consisting of four options (one correct) with a pass mark of 60%. Given that Outcomes 1 and 2 relate to raw knowledge and theory, this is an area to assess the learner's competency. The test could consist of a relatively high number of questions (30 or 40 for example), lasting an hour, which would span both of the outcomes and sample all of the associated knowledge statements (including at least one question for each statement). Additional types of questions should be considered, such as drag-and-drop and hotspot, etc.

The instrument of assessment for the **product evidence** could be a report or presentation. The report should include a description of the learner's activity and any potential findings. The product evidence should be produced independently by the learner.

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate). If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

There are opportunities to develop the Core Skill in *Communication*.

All outcomes require learners to be able to understand and communicate basic computing and IoT concepts. Outcomes 3 and 4 have a requirement for a report, with which the learner will develop communication skills.

Furthermore, it is expected the learner will naturally develop core and other essential skills whilst studying for this unit, such as analytical thinking, which will be required when they functionally decompose learning objectives.

Unit title: Internet of Things (SCQF level 7)

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when learners achieve the Unit, their Core Skills profile will also be updated to show they have achieved Critical Thinking at SCQF level 5.

History of changes to unit

Version	Description of change	Date
02	Core Skills Component Critical Thinking at SCQF level 5 embedded.	31/08/18

© Scottish Qualifications Authority 2018

This publication may be reproduced in whole or in part for educational purposes provided that no profit is derived from reproduction and that, if reproduced in part, the source is acknowledged.

Additional copies of this unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.

General information for learners

Unit title: Internet of Things (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit will provide you with knowledge in relation to the Internet of Things. This includes the basic concepts of the IoT, including history of the IoT and where it has come from; through to modern-day installation of IoT devices and the data they produce. You will also concentrate on the cyber security of and IoT device. You will develop writing and research skills whilst undertaking this unit.

The unit is split into four outcomes. The first two are theory and knowledge-based. The assessment for this will, most likely, be a closed-book assessment with multiple-choice questions of a similar nature. During the second half of the unit, you will develop practical skills. You will use IoT devices, either physically or through a simulated environment. The assessment for this will be an ongoing assessment and will (most likely) comprise a report, whereby you will describe your practical activities and report on your findings.

The cyber security of the IoT is growing in importance. There have been many attacks on companies that use live IoT devices. As a cyber-security professional, it is your job to make sure your IT infrastructure is fit for purpose and has the correct security in place to reduce the risk of any malicious activities.

On completion of this unit, you will be able to identify IoT concepts and will have developed knowledge of devices, implementations, protocols, security concerns and device security vulnerabilities of the IoT. You will also have a general understanding of networks and big data, allowing you to focus on cyber security, data science or network security.

After you complete this unit, you may progress to further HN studies in a related area, such as the HND in Cyber Security, or other areas.

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when you achieve the Unit, your Core Skills profile will also be updated to show you have achieved Critical Thinking at SCQF level 5.