Next Generation Higher National Unit Specification

Internet of Things (SCQF level 7)

Unit code: J692 47

SCQF level: 7 (8 SCQF credit points)

Valid from: session 2021–22

Prototype unit specification for use in pilot delivery only (version 1.0) May 2022

This unit specification provides detailed information about the unit to ensure consistent and transparent assessment year on year.

This unit specification is for teachers and lecturers and contains all the mandatory information required to deliver and assess the unit.

This edition: May 2022 (version 1)

Unit purpose

This unit introduces learners to the internet of things (IoT). It entails the history of IoT and where the concept has come from, through to modern-day IoT devices and real-world implementations. It focuses 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 and, more importantly, teach them 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.

When they have completed this unit, learners can identify IoT concepts and demonstrate their knowledge of devices, implementations, protocols, security concerns and device security vulnerabilities of the IoT. They can then progress to further HN units, especially those related to cyber security.

Unit outcomes

Learners who complete this unit can:

1 describe the IoT and its real-world implementations
2 explain IoT communication protocols and how data can be used
3 implement an IoT device to collect meaningful data
4 improve the security of an IoT device

Evidence requirements

Learners must provide both knowledge and product evidence.

Knowledge evidence

The knowledge evidence must relate to outcomes 1 and 2, and cover the knowledge required in these two outcomes. Learners must demonstrate the following knowledge:

- 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

Knowledge evidence can be written or oral or a combination of these. It can be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

Evidence is required for all knowledge and skills statements in outcomes 1 and 2 and can be sampled when a traditional test is used. If you use a test, you must do so under supervised conditions, with a controlled location and timing. Learners cannot access reference materials during tests.

Product evidence

The product evidence should cover outcomes 3 and 4, as these are more suited to practical and hands-on tasks.

Learners must choose, install and implement at least one IoT device to collect meaningful data. They can 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. Learners should produce evidence for outcomes 3 and 4 over a set period of time, and must do so independently. The assessment is carried out under open-book conditions, during which learners can access reference materials. Indeed, learners should make good use of referencing and linking to external information.

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

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

The ‘Additional guidance’ section provides specific examples of instruments of assessment that can generate the required evidence.

Knowledge and skills

The following table shows the knowledge and skills covered by the unit outcomes:

Knowledge	Skills
Learners should understand the: ♦ history of the IoT ♦ various industries that use the IoT ♦ common business models that use the IoT ♦ definition of a 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 the IoT ♦ common IoT themes ♦ examples of real-world implementations ♦ 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 ♦ types of data ♦ security vulnerabilities of a given IoT device ♦ outdated and vulnerable communication protocols ♦ security features to reduce the risk of an attack ♦ ways to make an IoT device more secure	Learners can: ♦ select an IoT device ♦ install the IoT device ♦ implement the chosen IoT device ♦ collect data from the IoT device ♦ analyse the collected data ♦ identify security vulnerabilities of a given IoT device ♦ recognise outdated and vulnerable communication protocols ♦ test security of an IoT device ♦ enhance the security of an IoT device

Meta-skills

Throughout the unit, learners develop meta-skills to enhance their employability in the computing sector.

Self-management

This meta-skill includes:

- integrity: ethics

Social intelligence

This meta-skill includes:

- communicating: receiving information, giving information
- feeling: social conscience

Innovation

This meta-skill includes:

- curiosity: questioning, information sourcing, problem recognition
- sense-making: pattern recognition, synthesis, analysis
- critical thinking: logical thinking, judgement, computational thinking

Literacies

Numeracy

Learners develop numeracy skills throughout the unit, and particularly as they develop their data-analysis skills.

Communication

Learners develop communication skills throughout the unit, and particularly when they produce a report or presentation on their findings and recommendations.

Digital

Learners develop digital skills and computer literacy throughout the unit, and particularly as they choose a suitable IoT to collect, analyse data and improve the security of an IoT device.

Delivery of unit

While the exact time allocated to this unit is at your discretion, the notional design length is 40 hours. One possible approach is to distribute the available time as follows:

Outcome 1 — Describe the IoT and its real-world implementations (10 hours)
Outcome 2 — Explain IoT communication protocols and how data can be used (10 hours)
Outcome 3 — Implement an IoT device to collect meaningful data (10 hours)
Outcome 4 — Improve the security of an IoT device (10 hours)

You can carry out summative assessment at any time. We recommend that if you use testing, you do this towards the end of the unit. If you use continuous assessment (for example, a blog), you can start early on in the unit and continue until the end.

You can carry out formative assessment at various stages in the unit. You can choose to do this at the end of each outcome to ensure that learners have grasped the knowledge it contains. You can then diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

Learners do not require previous knowledge or experience for this unit. However, they would benefit from an interest in modern-day computing, cyber security and networking. They can demonstrate this with a qualification 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.

If you deliver this unit as part of a group award, we recommend that you teach and assess it within the subject area of the group award to which it contributes.

Additional guidance

The guidance in this section is not mandatory.

Content and context for this unit

Please note that, in the following guidance relating to specific outcomes, we do not seek to explain each knowledge and skills statement, which we leave to you. Instead, we look to clarify the statement of standards where it is potentially ambiguous. We also focus on non-apparent teaching and learning issues that can be overlooked, or not emphasised, during unit delivery. As such, this guidance is not representative of the relative importance of each knowledge and skill statement.

Describe the IoT and its real-world implementations (outcome 1)

Outcome 1 takes a theoretical approach to the concept of IoT. We suggest that you cover the history of the IoT from the general creation of the concept, through to more modern-day installations. You should outline the different industries that are using the IoT for a specific reason. For example, an oil and gas company might use an IoT device to collect well pressure, while a local council might use an IoT device to monitor the amount of grit remaining in a street-side grit bin. You should provide an overview of a smart city and describe how everything could be connected to the IoT cloud or internet. You should focus on actual IoT hardware related to the topic, and encourage further discussion on the advantages and disadvantages of this.

Explain IoT communication protocols and how data can be used (outcome 2)

Outcome 2 also takes a theoretical approach. It looks at the data that an IoT device collects and how it can be used, and takes a computer-science approach as well as a networking view. You should spend time covering the main types of IoT communication protocols, such as Transmission Control Protocol (TCP) and/or User Datagram Protocol (UDP). You should describe the concept of IPv4 and IPv6 and, more importantly, how these two protocols play the most fundamental role within 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, there are distinct security implications.

Implement an IoT device to collect meaningful data (outcome 3)

Outcome 3 takes a hands-on approach to learning. We strongly encourage embracing this approach, but this remains at your discretion. Learners should research an IoT device and then physically install one. They should understand why one IoT device is chosen for a specific purpose over another. The installed IoT device should be able to collect and send meaningful data. Learners should analyse this data, then produce a report and statement about it. If your centre is unable to facilitate a physical estate of IoT devices, we suggest you do this virtually.

Improve the security of an IoT device (outcome 4)

Outcome 4 builds upon outcome 3, but focuses on the security of the device. Learners should focus on the range of security vulnerabilities of their IoT device and make notes on how to make the device more secure and robust. You should encourage discussion about outdated and insecure data communication protocols within this outcome.

Outcomes 3 and 4 are considered to be taught outcomes, where learners apply practical skills, and you should focus on learners working independently.

Due to the nature of IT and cyber security roles, we recommend that learners get hands-on lab time with IoT devices. If this is not possible, they can use a virtual or simulated environment.

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

Approaches to assessment

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 your learners.

We suggest that you deliver outcomes 1 and 2 together, and carry out summative assessment at the end of the first two outcomes. You can then move on to outcomes 3 and 4. These outcomes take a more hands-on approach, and asking learners to produce a report is more appropriate to this type of learning and delivery.

The assessment for the knowledge evidence is most likely to be a single assessment, covering outcomes 1 and 2. This could be a selected-response test consisting of four options (one correct) with a pass mark of 60 per cent. As outcomes 1 and 2 relate to raw knowledge and theory, assessment would determine learners' competence. The test could consist of a relatively high number of questions (for example 30 or 40). It could last 1 hour, spanning both outcomes and sampling all of the associated knowledge statements, including at least one question for each statement. You can also consider alternative question types, such as drag-and-drop and hotspot.

Product evidence could be a report or presentation. The report should include a description of the learner's activity and any potential findings and they should produce their product evidence independently.

A more contemporary approach to assessment would involve using a blog to record learning and the associated activities, throughout the life of the unit. Descriptions and explanations in the blog would provide knowledge evidence and product evidence could be in the form of video recordings, for example. You should assess the blog using defined criteria to allow 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.

You can use formative assessment to assess knowledge at various stages throughout the life of the unit, ideally 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 you use a blog for summative assessment, you could also use it to help you with formative assessment. Since learning and misconceptions would be apparent from the blog, you could intervene to correct misunderstandings as required.

Equality and inclusion

This unit is designed to be as fair and as accessible as possible with no unnecessary barriers to learning or assessment.

You should take into account the needs of individual learners when planning learning experiences, selecting assessment methods or considering alternative evidence.

Guidance on assessment arrangements for disabled learners and/or those with additional support needs is available on the assessment arrangements web page: www.sqa.org.uk/assessmentarrangements.

Information for learners

Internet of Things (SCQF level 7)

This section explains:

- what the unit is about
- what you should know or be able to do before you start
- what you need to do during the unit
- opportunities for further learning and employment

Unit information

This unit provides you with the basic concepts of the internet of things (IoT). This includes the history of the IoT and where it has come from, through to modern-day installation of IoT devices and the data they produce. You also concentrate on cyber security of IoT devices. This unit gives you opportunities to develop your writing and research skills.

It is split into four outcomes. The first two are theory and knowledge-based. Your assessment is most likely to be closed-book with multiple-choice questions of a similar nature. During the second half of the unit, you develop practical skills, and should have the opportunity to use IoT devices, either physically or in a simulated environment. Assessment for this is ongoing, and is likely to involve producing a report, where you 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. If you are 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 can identify IoT concepts and have developed knowledge of devices, implementations, protocols, security concerns and device security vulnerabilities of the IoT. You also have a general understanding of networks and big data, allowing you to focus on cyber security, data science or network security.

This unit also provides opportunities for you to enhance your meta-skills in self-management, social intelligence and innovation.

Administrative information

Published: May 2022 (version 1.0)

Superclass: CB

History of changes

Version	Description of change	Date

Note: please check SQA's website to ensure you are using the most up-to-date version of this document.