Higher National Unit Specification

General information

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

Unit code: J0HH 34

Superclass: CC

Publication date: June 2018

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to introduce learners to ethics and professionalism as they relate to cyber security. This is a **specialist** unit intended for those working, or wishing to pursue a career, in cyber security.

The unit covers a wide range of knowledge and skills relating to ethics and professionalism in this field, including the importance of personal privacy, intellectual property rights, digital rights management, corporate responsibility for data security and cyber resilience, and professional codes of practice relating to security professionals.

Learners will gain knowledge of contemporary legislation relating to data security and personal privacy; appreciate the ethical issues facing cyber security specialists; explore the importance of information policies; and find out about the professional bodies that represent security professionals.

This unit will provide a grounding in the ethical and professional standards expected to be practised by security professionals. Learners may progress to a wide range of cyber security units at the same or higher level.

Outcomes

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

1 Explain professionalism and ethics as they relate to cyber security.
2 Describe the role of security professionals in cyber security.
3 Explain contemporary legislation, standards and code of practice in relation to cyber security.

Higher National Unit Specification: General information (cont)

Unit title: Professionalism and Ethics in Cyber Security (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

While entry is at the discretion of the centre, learners would normally be expected to have an understanding of information technology within organisations.

Core Skills

There is no automatic certification of Core Skills or Core Skill components in this unit.

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.

The Assessment Support Pack (ASP) for this unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

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: Professionalism and Ethics in Cyber Security (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

Explain professionalism and ethics as they relate to cyber security.

Knowledge and/or skills

- Historical development of moral philosophy
- Definitions of ethics and professionalism
- Benefits of ethics to society
- Benefits of privacy to individuals
- Business benefits of ethics and professionalism
- Importance of professional standards to employers
- Ethical considerations in cyber security
- Conflicting objectives in security and privacy, and ethics and profitability

Outcome 2

Describe the role of security professionals in cyber security.

Knowledge and/or skills

- Information governance including information policies
- Job roles in cyber security
- Professional bodies relevant to security professionals
- Corporate responsibilities for protecting data
- Corporate responsibilities for cyber resilience
- Personal, professional and corporate costs of data breaches
- Ethical issues faced by cyber security specialists

Outcome 3

Explain contemporary legislation, standards and code of practice in relation to cyber security.

Knowledge and/or skills

- Legislation relating to privacy, data management, and digital rights management including criminal penalties and financial and reputational costs of breaches
- Policies and standards that impact on security professionals
- National and international codes of practice in relation to cyber security

Higher National unit specification: Statement of standards (cont)

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

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 **one** form.

1 Knowledge evidence (Outcomes 1, 2 and 3)

The **knowledge evidence** will relate to all outcomes (1–3). Knowledge evidence is required for **all** knowledge and/or skills statements in these outcomes. The evidence may be produced over an extended period of time in lightly controlled conditions. The amount of evidence may be the **minimum** required to infer competence. For example, a brief treatment of moral philosophy is acceptable (Outcome 1); only the main job roles (Outcome 2) are required; it is sufficient to explain the most important standards (Outcome 3). The evidence must include:

- Description of **at least two** professional bodies relevant to security professionals
- Description of **at least three** areas of legislation relating to cyber security professionals
- Evaluation of **at least three** ethical issues faced by cyber security specialists
- **At least two** examples of a code of practice, either national or international, for cyber security professionals

The knowledge evidence may be sampled when testing is used. In this case, the evidence must be produced under controlled conditions in terms of location (supervised), timing (limited) and access to reference materials (not permitted). The sampling frame must include all outcomes (at least partially) and the majority of knowledge/skills statements (in each outcome). The sampling frame must always include the following:

- Benefits of ethics to society
- Business benefits of ethics and professionalism
- Ethical issues faced by cyber security professionals

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). Particular consideration should be given to digital formats and the use of multimedia.

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: Professionalism and Ethics in Cyber Security (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

In recent years, there has been an increase in demand for cyber security professionals due to the increase in cyber-attacks. The purpose of this unit is to introduce learners to ethics and professionalism as they relate to cyber security. This is a **specialist** unit intended for those working, or wishing to pursue a career, in cyber security.

The unit covers a wide range of knowledge and skills relating to ethics and professionalism in this field, including the importance of personal privacy, intellectual property rights, digital rights management, corporate responsibility for data security and cyber resilience, and professional codes of practice relating to security professionals.

Learners will gain knowledge of contemporary legislation relating to data security and personal privacy; appreciate the ethical issues faced by cyber security specialists; explore the importance of information policies, and find out about the professional bodies that represent security professionals.

This unit will provide a grounding in the ethical and professional standards expected to be practised by security professionals. Learners may progress to a wide range of cyber security units at the same or higher level.

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: Explain professionalism and ethics as they relate to cyber security.

This outcome prepares the learner in understanding the importance of professionalism and ethics within cyber security. The historical development of moral philosophy should be covered briefly as an introduction to this outcome. Learners must define ethics and professionalism as they relate to cyber security. Learners should be able to discuss the benefits of ethics to society and businesses.

Also, discussion of real organisational/workplace environments and staff roles should be encouraged in relation to all outcomes for the unit.

Higher National Unit Support Notes (cont)

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

Outcome 2: Describe the role of security professionals in cyber security.

This outcome gives the learner an understanding of the different roles within cyber security and the issues professionals are facing when working. Learners should gain some knowledge of information governance, covering aspects such identifying and classifying information assets and processes at risk (ie, what needs to be protected); assessment of risks (confidentiality, integrity, availability); threats (opportunity, ability, motive) and associated impact. However, these only need to be introduced at a high level. Learners should briefly explore the roles of cryptography and identity in cyber security.

Learners should investigate the role of professionals working in cyber security and be able to identify different roles in cyber security, as well as the different professional bodies that are relevant within the industry. Learners should be able to describe the differences between cyber security and cyber resilience and describe how employers have responsibility for protecting the data they collect.

Outcome 3: Explain contemporary legislation, standards and code of practice in relation to cyber security.

This outcome aims to give the learner an understanding of legislation and policies relating to security personnel. Learners should be able to explain legislation relating to privacy, data management, and digital rights management, including criminal penalties and the financial and reputational costs of breaches. Learners should be able to identify policies, codes of practice and standards that are relevant and explain the importance of them to security professionals.

Useful links

- **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf**
- **https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework**
- **https://www.iisp.org/imis15/iisp/About_Us/Our_Mission/iispv2/About_us/Our_Mission.aspx?hkey=9a43cc5c-8b71-4770-bfa9-d60e5c7b3ba9**
- **http://www.issa-uk.org/**
- **https://southwalescyber.net/ncscs-new-professional-body-cyber-security-14th-november-2017/**
- **https://www.ncsc.gov.uk/scheme/gchq-certified-training**

Higher National Unit Support Notes (cont)

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

Guidance on approaches to delivery of this unit

It is recommended that Outcomes 1 and 2 are taught sequentially, with Outcome 3 being taught alongside.

There are many different delivery methods that can be used for this unit. For example, presentations, demonstrations and practical exercises can be used as well as the use of film, video and podcast. However, when this approach is used, it is vital that the tutor provides the context, sets objectives along with experiences and outcomes, and regularly reviews progress. Group discussions and other collaborative techniques are encouraged.

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

Outcome 1: 15 hours
Outcome 2: 15 hours
Outcome 3: 10 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements) it is recommended that this is 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.

A traditional approach to assessment would involve a test for all outcomes. The test could be a multiple-choice assessment. The test could consist of a number of Selected Response Questions (SRQs) that assess the knowledge and understanding contained in Outcomes 1, 2 and 3. The test would be timed, closed-book and supervised. An appropriate pass mark would be set. Learners who achieve this threshold would achieve the three outcomes. The majority of questions would relate to factual recall (professional bodies relevant to cyber security); some questions would relate to deeper understanding and would require more complex types of questions.

Alternatively, the evidence could be generated by using a smaller number of short-answer questions, which could be written or oral. These questions could cover multiple concepts in each question and, therefore, would require fewer questions.

It is recommended, however, that the evidence for all three outcomes is gathered holistically through a project-based assessment, where learners would work from a given case study/scenario of a realistic environment that cyber professionals would be working in. The evidence could take an appropriate form, such as OneNote, wiki, blog or e-portfolio based on given case studies. However, other forms of evidence may also be acceptable if they demonstrate a good understanding of all the outcomes.

Work produced will be under supervised open-book conditions. E-assessment could be used as an alternative to allow learners to provide a digital record of evidence to demonstrate knowledge and/or skills. A detailed case study should be given to learners close to the start of the unit to allow students to relate the knowledge and/or skills within the teaching/learning to a workplace context.

The assessment would be open-book and, therefore, learners should be encouraged to gather and refine information/knowledge related to the range stated for each outcome. The final assignment work produced by learners should be evaluated on the basis of the evidence requirements stated for the unit. Appropriate measures should be taken to ensure the integrity of individual student assignment submission.

Regardless of the instrument of assessment chosen by the centre, the undernoted identifies the minimum criterion for awarding a pass for the unit:

- Describe a minimum of two professional bodies relevant to cyber security professionals
- Describe three areas of legislative concern for a specified cyber security professional role
- Evaluate three ethical issues cyber security personnel may face and suggest an appropriate resolution to a specified area of ethical conflict
- Give at least two examples of a code of practise, either national or international, for cyber security professionals and how this helps them in their work

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.

Higher National Unit Support Notes (cont)

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

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

Learners will have the opportunity to develop aspects of the Core Skill of *Communication* at SCQF level 6 as they work through the assessment requirements. Additional opportunities could be realised through the chosen methods of delivery of the unit and integrated learner activities.

History of changes to unit

Version	Description of change	Date

General information for learners

Unit title: Professionalism and Ethics in Cyber Security (SCQF level 7)

The purpose of this unit is to introduce you to ethics and professionalism as they relate to cyber security.

The unit covers a wide range of knowledge and skills relating to ethics and professionalism in this field, including the importance of personal privacy, intellectual property rights, digital rights management, corporate responsibility for data security and cyber resilience, and professional codes of practice relating to security professionals. The unit is designed to allow you to gain the knowledge and understanding required to carry out the day to day duties and activities required of a cyber security professional in an ethical manner with due attention to business, society and legal requirements. The unit consists of three outcomes that inter-relate to one another, to assist you in development of a knowledge base and understanding of the responsibilities of a cyber security professional with regard to:

- Importance of professionalism and ethics to society and businesses
- Professional bodies relevant to security professionals and the importance of professional standards
- Information governance
- Ethical issues faced by cyber security specialists
- Contemporary legislation relating to privacy, data management and digital rights management
- National and international codes of practice in relation to cyber security

The unit is mainly theoretical. The assessment for all three outcomes will, most likely, be gathered holistically through a project-based assessment, where you will have the opportunity to work from a given case study/scenario of a realistic environment that cyber professionals would be working in.

The knowledge gained through researching the areas included in the unit will enable you to approach future job roles in the cyber security profession in a responsible and ethical way. Also, throughout the unit you will have opportunities to develop aspects of the Core Skill of *Communication* at SCQF level 6.

This unit will give you a grounding in the ethical and professional standards expected to be practised by security professionals. On successful completion of the unit, you may progress to a wide range of cyber security units at the same or higher level.