National Unit specification

General information

Unit title: Data Security (SCQF level 6)

Unit code: H9E2 46

Superclass:	CC
Publication date:	September 2015
Source:	Scottish Qualifications Authority
Version:	02

Unit purpose

The purpose of this Unit is to explore current practice in corporate data security, and learn techniques for the development of a business security strategy.

A specific aim of this Unit is to equip learners with knowledge and skills to create a data security policy for a professional organisation, and justify policy decisions based on best practice. Learners will be able to discuss the ethical, legal and professional aspects of the policy.

On completion of this Unit, learners will have practical experience of the risks associated with data security, and the knowledge and skills to develop a security strategy. Learners may progress to National Certificates or Higher National Certificates in Computing or related qualifications.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF 6.

Outcomes

On successful completion of the Unit the learner will be able to:

1 Analyse the approach to data security made by organisations.
2 Investigate technologies and strategies used by businesses to protect customer data.
3 Create a security strategy for a small business

National Unit specification: General information (cont)

Unit title: Data Security (SCQF level 6)

Credit points and level

1 National Unit credit at SCQF level 6: (6 SCQF credit points at SCQF level 6)

Recommended entry to the Unit

Access to this Unit will be at the discretion of the centre. The *Data Security* Unit levels have been designed to work together and while it is recommended that the learner has achieved the *Data Security* Units at SCQF levels 4 and 5, it is not a mandatory requirement.

Depending on the teaching approach access to the internet and basic browser search abilities will be helpful and a basic understanding of IT and computer security concepts would help in the successful completion of this Unit.

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 6 Planning and Organising at SCQF level 6

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

Context for delivery

This Unit may be offered stand-alone or as part of the National Progression Award in Cyber Security at SCQF level 6. If offered as part of this Group Award, there may be opportunities to combine and integrate teaching and learning across Units. There may also be opportunities to combine Evidence Requirements and integrate assessments.

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**.

National Unit specification: Statement of standards

Unit title: Data Security (SCQF level 6)

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.

Outcome 1

Analyse the approach to data security made by organisations.

Performance Criteria

(a) Explain the cyber security challenges faced by small, medium and large companies.
(b) Explain the cyber security challenges faced by different sectors.
(c) Identify sources of best practice in cyber security.
(d) Identify different types of security personnel and their roles in small, medium and large companies.
(e) Compare physical, perimeter and internal network security.
(f) Explain the importance of cyber resilience.
(g) Investigate approaches to good business cyber security.

Outcome 2

Investigate technologies and strategies used by businesses to protect customer data.

Performance Criteria

(a) Identify the major suppliers in the cyber security goods and services sectors.
(b) Define current types of technology used for cyber security defence.
(c) Explain how current defence technology works and the associated risks.
(d) Explain the importance of patching and why software needs regularly patched.
(e) Explain table top exercises and their purpose.
(f) Explain real life strategies used by businesses to protect customer data.

Outcome 3

Create a security strategy for a small business.

Performance Criteria

(a) Define the cyber security risks faced by small businesses.
(b) Explain potential solutions to cyber security risks faced by small businesses.
(c) Create a security strategy for a small business.

Unit title: Data Security (SCQF level 6)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. However, sampling may be used in certain circumstances (see below).

The evidence for this Unit 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.

Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the learner. Authentication must be used where this is uncertain.

Evidence is required for two types of competence: evidence of **cognitive competence** (knowledge and understanding) and evidence of **practical competence** (practical abilities).

The evidence of cognitive competence must include Outcome 1 (all Performance Criteria), Outcome 2 (all Performance Criteria) and Outcome 3 (PC (a) and (b)).

Cognitive competence may be sampled across the knowledge domain defined by this Unit specification, so long as the sample is unknown, and unpredictable, to the learner. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set.

The cognitive competency component will provide the knowledge and understanding needed to equip the learner with the ability to complete the practical nature of Outcome 3 which will form the main Evidence Requirement.

The evidence of practical competence for this Unit will relate to Outcome 3 (PC (c)) and the creation of a robust cyber security strategy for **at least one** small business. The strategy can take a variety of forms but the candidate should be able to defend the approach they have made based on their knowledge from Outcomes 1 and 2.

It is anticipated that the Outcome 3 would take the form of a practical project, defended in a peer environment. However, other forms of evidence that demonstrate good understanding of Outcomes 1 and 2 are also acceptable.

Re-assessment is possible if the strategy is found to have deficiencies either through written or oral means.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provide specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Data Security (SCQF level 6)

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

The general context for this Unit is to introduce learners to strategies used by industry to protect their customers' data from loss or theft due to cyber-attack. There are key differences in how this is achieved compared to individuals protecting their own data and this Unit should give the learners a good grounding in the ways this can be achieved.

Outcomes 1 and 2 should provide a background to how businesses protect themselves from data loss due to cyber-attack. Outcome 3 will apply these skills in a requirement to write a cyber security strategy which will provide good cyber security protection and most importantly *resilience* for a fictitious small company.

Throughout this Unit learners must adhere to basic ethical standards of practice.

Outcome 1

This Outcome covers the approaches made by industry to protect themselves. Companies of different sizes and different sectors have different risks and thus will have different defence strategies. The Outcome also encourages the learners to investigate where they might get access to current best practice which they will need for Outcome 3. Commonly accepted best practice can be found on the UK Government's published ten step guide and is a very useful starting place for up to date information.

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

Learners will be required to appreciate the inherent risks associated with any networked device, and understand the potential threats posed by public and private IP addresses and TCP ports.

The learners will also start to get an understanding of the types of roles companies have for security personnel and how their jobs differ. For example a small business might have only one person who manages everything whereas large companies may have many people, eg CISOs, forensic analysts, education specialists. Large companies may also outsource security testing to specialist penetration testing companies who will test both perimeter and internal defences. This may include an attempt to get physical access to the building.

Unit title: Data Security (SCQF level 6)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

Resilience is a key aspect to security. It is generally accepted that most company perimeters will be breached by a determined attack, however all companies should be resilient from the point of view of how quickly can they spot and recover from an attack.

A good strategy for making a company more resilient with limited funding is to recognise what the 'crown jewels' are. This means identifying what is absolutely crucial to the continued existence of a company and what can be sacrificed or less well guarded. An example of crown jewels might be the central database. In this example it should be comprehensively protected whilst the corporate website is less important.

Outcome 2

This Outcome should equip the learner with knowledge of the tools that are available to defend a business from cyber-attack.

The learner should have a good understanding of who the main companies on the market are and what products they sell. This should be for goods, ie technology and services, eg penetration testing and forensic analysis companies.

The learners should also know about the main types of cyber security defence technology and have a broad understanding of how they work, eg Firewalls and honey traps.

One of the main reasons that systems get breached is because they are not patched in a timely fashion. This means that known exploits can be commoditised and systems easily compromised.

Table top exercises are used to test the readiness and resilience of companies defence to cyber-attack. Learners should understand how useful these exercises can be and how they might be implemented. It is suggested that a good way to do this is to act out a cyber-attack with learners taking different roles and evaluating what worked and what did not after the event.

Outcome 3

In this Outcome the learners should discuss the specific dangers faced by small to medium sized companies, it might be useful to discuss the well-known cyber victim, eg target and discuss why it failed.

The learners should be able to demonstrate how they would protect a fictitious small business. It is anticipated that this would take the form of a project where the learner first invented a company, defining the sector and the security team and imagine that the CEO has asked for a security strategy on a limited budget. Drawing on experience from Outcomes 1 and 2 the learners should adhere as far as possible to current best practice and be able to identify what needs protected and where the risks remain. The plan could be presented back to the class in the form of the security manager discussing his conclusions with the CEO.

Unit title: Data Security (SCQF level 6)

Soft skills are regularly seen as a key attribute by employers so in this Outcome it is intended that learners are helped to discuss a complicated subject at a level that a CEO can understand and ultimately support.

It may be useful to bring a real CEO where possible to grade the security strategies and soft skills.

Guidance on approaches to delivery of this Unit

A practical, hands-on approach to learning should be adopted in order to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities.

At this level, learning should be a mix of tutor-led and learner-led. It is anticipated that some initial introduction and explanation will be required for each Outcome. However, there is significant scope for learners to research and explore the topics once this initial seeding has taken place. Tutors should expect some independent learning to take place and support students with this where appropriate.

Outcomes 1 and 2 can be delivered in any order, however it is suggested that both 1 and 2 are completed before Outcome 3 is attempted. The reason for this is that Outcome 3 is mainly learner led and can only be successfully completed with knowledge gained from Outcomes 1 and 2.

The distribution of time over the three Outcomes is at the discretion of the centre and thus will be influenced by a number of factors. However a possible distribution is as follows:

Outcome 1:	12 hours
Outcome 2:	12 hours
Outcome 3:	16 hours

A significant proportion of the time is given to Outcome 3 because of the practical nature of the Outcome.

The Unit is wholly concerned with data security in industry. Many businesses are keen to get involved with education and it is recommended that where possible, real examples are used by collaborating with local industry. Encourage learners to keep up to date with international media reports of data security failings and educators are encouraged to use the internet to find current examples of best practice.

The following website is a good resource:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 6)

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.

The evidence for knowledge and understanding in Outcomes 1, 2 and 3 (PC (a) and (b)) can be captured in various ways, such as reports, presentations, videos, podcasts or summaries of learning. A traditional test which appropriately samples knowledge is also acceptable.

It is possible that the security strategy, produced in Outcome 3 (PC (c)) would adequately cover all the Performance Criteria for all the Outcomes assuming that significant background information was given before the solution was provided.

The evidence for Outcome 1 could take the form of an essay describing common approaches to cyber security in industry. All the Performance Criteria should be covered in the content of the essay and should make reference to national standards in cyber security and fully referenced.

The evidence for Outcome 2 could take the form of a case study into the security strategy of a large company. This may be best exposed by using the example of a large company that has suffered a public cyber-attack and exploring the circumstances around why the security strategy of the company was not sufficient to prevent the attack.

The evidence for Outcome 3 could be the simulation of a presentation of a costed security strategy to a CEO. There should be opportunities to challenge decisions and assumptions made in the candidate’s report. The strategy should reference current best practice yet be sufficient to the company's needs. Soft skills are a key requirement of industry and the ability to present the strategy in a way that an executive board can understand should be a factor in the assessment.

Another way of assessing Outcome 3 would be to present the strategy as a document. The contents of the document can be assessed against best practice and Performance Criteria detailed in the Outcomes.

Another approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would log, on a daily or weekly basis, what candidates learn and what they do. However, their posts would have to satisfy the relevant Performance Criteria. Practical activities could also be recorded via the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities. When necessary, separate authentication (such as oral questioning) could be used for verification purposes.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 6)

The critical aspect is that the blog is an overall accurate reflection of the practical activities (and, therefore, the associated skills) carried out by the learner during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

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

The Unit provides opportunities to deliver some of the following Core Skills:

Information and Communication Technology (ICT) (SCQF level 6)
Communication (SCQF level 6)
Working with Others (SCQF level 6)

Some of the Core Skills components in *Communication* can be addressed in this Unit. There are opportunities to pick out important ideas and key points, choose a format, include information or ideas, present information and use spelling, grammar and punctuation to make your writing clear. Additionally, opportunities to express ideas or opinions clearly and in a logical way whilst listening to other and respond accordingly.

One or more of the Core Skills components in *Working with Others* can be addressed in this Unit. There are opportunities to carry out a role in a co-operative activity, and seek and offer support.

In addition to Core Skills, this Unit provides opportunities to develop digital citizenship skills.

This Unit has the Critical Thinking and Planning and Organising components of Problem Solving embedded in it. This means that when candidates achieve the Unit, their Core Skills profile will also be updated to show they have achieved Critical Thinking at SCQF level 6 and Planning and Organising at SCQF level 6.

History of changes to Unit

Version	Description of change	Date
02	Core Skills Components Critical Thinking and Planning and Organising at SCQF level 6 embedded.	09/09/2015

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: Data Security (SCQF level 6)

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 help you to explore current practice in corporate data security, and learn techniques for the development of a security strategy for a small business. Cyber-attack is a threat to businesses of all sizes and the economy of the UK which is why it has been made a Tier 1 threat by the UK Government.

The Unit is designed for those with a reasonable grounding in cyber security concepts. It covers best practice in data security within industry and intends to equip you with the ability to help a small company to set up their own cyber security strategy. Cyber security is evolving at a fantastic rate and it is therefore expected that you will have to research what the current state of the art is. This Unit will help you to identify the best places to find these resources.

The assessment may take on different forms. It may involve a short test of your knowledge or application of your learning in a mock environment.

On completion of this Unit, you will have practical experience of developing a security strategy for a small business. You may progress to National Certificates or Higher National Certificates in Computing or related qualifications or Modern Apprenticeships in Cyber Security.