****

**Assessment Strategy**

|  |  |
| --- | --- |
| **Sector** | **Digital Technology** |
| **Qualification Title(s)** | **Diploma in Digital Technology at SCQF Level 8** |
| **Developed by** | **Skills Development Scotland** |
| **Date approved by ACG** | **16 March 2022** |
| **Version** | **2** |

****

**Appendix: Assessment Strategy for the Diploma in Digital Technology at SCQF Level 8**

**(in support of the Overarching Assessment Strategy for competence-based qualifications)**

**Produced by: Skills Development Scotland**

**Approved by: Accreditation Coordination Group**

**Date: 16/03/2022**

**Contents**

[1. Purpose and use 1](#_Toc99447886)

[2. Generic requirements 2](#_Toc99447887)

[2.1 Workplace assessment 2](#_Toc99447888)

[2.2 Simulation in a realistic work environment 3](#_Toc99447889)

[3. Meta-skills 7](#_Toc99447890)

[4. Methods of assessment 7](#_Toc99447891)

# 1. Purpose and use

This document is an appendix to the Overarching Assessment Strategy for Competence-based Qualifications. This sets out the requirements that are specific to assessment of the qualification and covers the arrangements for the use of simulation and guidance on unit assessment for the Diploma in Digital Technology at SCQF Level 8.

The purpose of this appendix is to provide awarding bodies with an appropriate and consistent approach to assessment contextualised and exemplified for digital technology. It should be used as the basis for developing and defining evidence requirements and assessment methods for the qualification.

There are three pathway options that are available as part of the Diploma in Digital Technology at SCQF Level 8 qualification. These are as follows:

* Diploma in Digital Technology: Data Analytics at SCQF Level 8
* Diploma in Digital Technology: Software Development at SCQF Level 8
* Diploma in Digital Technology: Cyber Security at SCQF Level 8

These pathways incorporate both common units and pathway specific technical units that underpin overall competence in the workplace.

# 2. Generic requirements

## 2.1 **Workplace** assessment

*This outlines the guidance for assessing performance in the workplace.* *To be used in addition to the Overarching Assessment Strategy for Competence-based Qualifications. In the area of Digital Technology the following applies:*

The digital technology qualification will primarily be delivered and assessed in the workplace. This is the environment in which the learner will routinely be engaged in applying digital technologies to support their own organisation in developing and delivering customer products and services and organisational processes through the application of digital technologies. This qualification is designed to recognise competence in the application of digital technologies in different sectoral contexts.

This requires that the learner is engaged in a digital technology role and that work-based learning is aligned to and assessed against qualification unit performance requirements and knowledge and understanding requirements. This is the primary method by which learners develop and evidence the performance, knowledge and understanding requirements and meta-skills set out in the qualification.

Work-based learning is a partnership between learner, employer and learning provider and all learners must have the support of an employer in undertaking the qualification.

The Overarching Assessment Strategy identifies sources of evidence of learner competence. In addition, for assessment of digital technology qualifications, other types of evidence have been identified. These are listed in section 4.

.

## 2.2 Simulation in a realistic work environment

*In addition to the Overarching Assessment Strategy in relation to the use of simulation for assessment, in the area of Digital Technology the following applies:*

Simulation is permissible only as set out in section 2.1 of the overarching Assessment Strategy for competence-based qualifications *and* as set out in this section. The digital technology workplace is ubiquitous across a wide range of sectors. It encompasses digital technologies that can interact with commercial or sensitive data that is used to support the delivery of products and services. In such cases the opportunities for workplace assessment may be restricted and learners may not be able to use live environments or data as sources of evidence for digital technology workplace assessment. There may, therefore, be some circumstances within the units where assessment can only be carried out using simulation. These include where:

* digital technology activities are based on live digital and data environments and where mistakes made in carrying them out would pose unacceptable risks to the organisation and / or its customers (e.g. in certain digital technology cyber security and data environments)
* the costs incurred would be unacceptably high if mistakes were made during a digital technology assessment activity (e.g. operating with complex digital technology infrastructure)
* situations where the qualities and outcomes of the learner’s behaviour are almost impossible to distinguish from those of their peers or colleagues, making authenticity uncertain (e.g. in some collaborative digital technology teamwork contexts)
* digital technology activities or situations which are sufficiently unusual and infrequent (e.g. processes such as an initial configuration or deployment of cyber security control implementations).
* when the collection and/or review of evidence of workplace performance would intrude unacceptably on personal privacy or confidentiality (e.g. in some data, software and cyber security settings under GDPR, or where the digital technology context is subject to personal information such as healthcare or financial etc)
* a requirement to work with new techniques and/or work practices which may not be available in all workplaces (including cyber security e.g. digital forensics).

**Please note** that where realistic work environment conditions are applied these will require working conditions to be replicated for example, in line with timescales, customer requirements etc. Where simulation is carried out it is not expected to be used for full units.

**Recommended digital technology units where simulation would be suitable.**

The following tables indicate which digital technology units are appropriate for simulation as part of unit assessment methods.

**Mandatory common units across all digital technology pathways**

|  |  |  |  |
| --- | --- | --- | --- |
| *Developer Code* | *Unit Title* | *Mandatory/optional /additional* | *Permissible for simulation and rationale* |
| SDS 187 | Supporting digital business transformation | Mandatory | Not permissible for simulation |
| SDS 007 | Applying methods and principles in project management’ | Mandatory | Not permissible for simulation |
| SDS 012 | Developing meta-skills and personal professionalism | Mandatory | Not permissible for simulation |

*Table 1 – Guidance on the use of simulation for common units*

**Data analytics pathway units**

|  |  |  |  |
| --- | --- | --- | --- |
| *Developer Code* | *Unit Title* | *Mandatory/optional /additional* | *Permissible for simulation* *and rationale* |
| SDS 024 | Managing data assets | Mandatory | Not permissible for simulation |
| SDS 026 | Planning data analysis | Mandatory | Not permissible for simulation |
| SDS 022 | Locating and accessing data sources | Mandatory | Accessing live data sources may be problematic in a live production environment. These could be equally simulated offline to provide a realistic and safe environment for locating and accessing them. |
| SDS 032 | Transforming data for analysis | Mandatory | Transforming data is an offline activity, but may be exposed to sensitive or private information, so alternative simulated data sets could be used that present the same rigour and evidence of competence in a safe environment. |
| SDS 013 | Analysing data | Mandatory | Analysing data is an offline activity, and can be subject to sensitive or private information, so alternative simulated data sets could be used for analysis that present the same rigour and evidence of competence in a safe environment. |
| SDS 016 | Visualising and communicating data | Mandatory | Visualising data is an offline activity, and can be subject to sensitive or private information, so alternative simulated data sets could be used for visualisation that present the same rigour and evidence of competence in a safe environment. |
| SDS 020 | Implementing machine learning models | Additional | Implementing machine learning involves placing these algorithms into live production environments. This could have an impact on live data sets and may require static or dynamic streamed data sets depending upon the context. This would likely present too high a risk for most employers and so machine learning can be undertaken in a simulated sandbox, or offline development environment. There is the potential for real or simulated data sets to be used as training data depending upon local circumstances in a safe environment. |

*Table 2 – Guidance on the use of simulation for data analytics pathway units*

**Cyber security pathway units**

|  |  |  |  |
| --- | --- | --- | --- |
| *Developer Code* | *Unit Title* | *Mandatory/optional /additional* | *Permissible for simulation and rationale* |
| SDS 029 | Contributing to cyber security risk assessment and risk management | Mandatory | Not permissible for simulation |
| SDS 014 | Contributing to intrusion detection activities | Mandatory | Intrusion detection involves scanning live network and application environments to discover evidence of intrusion events and qualify them. It is possible to develop competency in intrusion detection using known intrusion events planted into simulated environments. In this way a variety of intrusion events that may rarely occur in real life, but which need to be identified and dealt with promptly to avoid serious impact can be undertaken to prepare learners to deal with them should they occur in a live environment. |
| SDS 027 | Providing incident management and response | Mandatory | Incident management involves responding to events as they occur. Therefore, it is possible to develop competency using the deployment of known incident events into simulated environments. |
| SDS 028 | Supporting security audit and compliance checking | Mandatory | Not permissible for simulation |
| SDS 017 | Delivering threat intelligence | Optional | Not permissible for simulation |
| SDS 015 | Contributing to scoping and implementing security testing | Optional | Security testing involves scanning live network and application environments. Vulnerability scanning and assessment searches systems for known vulnerabilities. Penetration testing attempts to actively exploit weaknesses in an environment.  It is accepted practice to develop competency in security through deploying vulnerabilities and exploits into simulated environments where this is not practical in live environments. |
| SDS 023 | Maintaining security operations | Optional | Security operations includes handling operating system updates, maintaining patch management, firewall and anti-malware update plans and implementing security controls. It will not always be practical to implement controls including patches and updates into live environments as this could risk their normal operation, and so the potential of undertaking off-line updates and testing of controls would provide the same rigour and evidence of competence in a safe environment. |
| SDS 025 | Performing digital forensic analysis | Optional | Digital forensics includes preserving evidence and analysing a range of digital technology systems to recover data. These include networks, computers, laptops, tablets, mobile phones, storage and other devices. These would be live devices in live environments and so from a learning perspective undertaking off-line digital forensic analysis with prepared scenarios would provide the same rigour and evidence of competence in a safe environment. |

*Table 3 – Guidance on the use of simulation for cyber security pathway units*

**Software development pathway units**

|  |  |  |  |
| --- | --- | --- | --- |
| *Developer Code* | *Unit Title* | *Mandatory/optional /additional* | *Suitability for simulation* |
| SDS 021 | Implementing software methodology | Mandatory | Not permissible for simulation |
| SDS 018 | Designing software | Mandatory | Not permissible for simulation |
| SDS 019 | Developing software | Mandatory | Not permissible for simulation |
| SDS 031 | Providing software testing and assurance | Mandatory | Not permissible for simulation |
| SDS 030 | Providing user and software documentation | Mandatory | Not permissible for simulation |

*Table 4 – Guidance on the use of simulation for software development pathway units*

# 3. Meta-skills

A key aspect of the digital technology qualification is that learners develop the range of meta-skills as identified in the Overarching Assessment Strategy (section 3.).

The unit *Developing meta-skills and personal professionalism* specifically requires learners to be able to achieve the following learning outcome:

* To develop meta-skills and personal professionalism through reflective practice, goal setting and active learning to improve own performance in line with organisational requirements.

This unit will draw on the assessment of other units in the qualification. Therefore, assessment of the performance and knowledge and understanding requirements is likely to integrate well with the assessment of the other units as opposed to being delivered as a standalone unit.

Assessment should focus on the nature and quality of the self-reflective practices and self-evaluation activities being undertaken, rather than the achievement or evidence of specific meta-skills. However, supporting evidence that examples the meta-skills development referred to in the self-reflective and self-evaluation practices should be provided.

Further information on meta-skills, including how meta-skills align to the units in this qualification can be requested from Skills Development Scotland at [apprenticeshipdevelopment@sds.co.uk](mailto:apprenticeshipdevelopment@sds.co.uk).

# 4. Methods of assessment

Learners are expected to demonstrate that they have met the performance requirements and knowledge and understanding requirements of this qualification and are competent in a digital technology role in line with one of the pathways available. Learners will gather evidence of their competence in the workplace and this will be assessed within an awarding body approved centre by qualified and experienced staff.

A range of assessment methods have been identified through the design of the digital technology qualification at SCQF level 8. Learners are expected to provide evidence of meeting the learning outcomes and the knowledge, skills and behaviours required to demonstrate that they are competent in the workplace. It is important for learners to recognise how they have developed skills and understanding along the way, and where these still need to be developed.  The following methods have been identified as particularly suitable for this qualification.

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment methods** | **Cyber Security** | **Data Analysis** | **Software Development** |
| Cross organisation projects |  | **X** |  |
| Case studies |  | **X** |  |
| Professional discussion | **X** | **X** | **X** |
| Portfolio of evidence | **X** | **X** | **X** |
| Problem based learning | **X** | **X** | **X** |
| Presentations | **X** | **X** | **X** |
| Security testing and digital forensic analysis | **X** |  |  |
| Realistic simulation via scenarios/questionnaires | **X** |  |  |
| Gamification | **X** |  |  |
| Catch the flag exercises | **X** |  |  |

*Table 5 – Assessment methods identified to support each of the digital technology pathways*

It is therefore recommended that learners undertaking the Diploma in Digital Technology at SCQF Level 8 qualification develop a portfolio of work to evidence their competence. This approach will allow the learner to collect evidence of achievement in ways that are most appropriate to the digital qualification pathway being studied.

It is a general requirement that Awarding Body arrangements ensure that digital technology competence can be demonstrated over a period of time, rather than simply for the purposes of a single assessment.

Performance evidence alone will not provide enough evidence of competence in this area. In particular, where the learner’s knowledge and understanding is not apparent from performance evidence, it must be assessed by other methods and be supported by suitable evidence.

Knowledge and understanding can be demonstrated in a number of different ways, but it is suggested that the most appropriate methods for this qualification are professional discussion and reflective accounts. Assessors should ask enough questions to be able to determine that the learner has an appropriate level of knowledge and understanding as required by the unit(s).