****

**Appendix: Assessment Strategy**

**Diploma in Digital Technology at SCQF Level 6**

**and**

**Diploma in Digital Technology at SCQF Level 8**

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

**Version 2**

**Produced by: Skills Development Scotland**

**Approved by: Accreditation Coordination Group**

**Date: 07/12/2022**

**Contents**

[1. Purpose and use 1](#_Toc118968242)

[2. Generic requirements 2](#_Toc118968243)

[2.1 Quality assurance requirements 2](#_Toc118968244)

[2.2 Occupational expertise and qualification requirements for those assessing or undertaking quality assurance of assessment 2](#_Toc118968245)

[2.3 Evidence requirements for assessment 2](#_Toc118968246)

[2.4 Simulation in a realistic work environment 2](#_Toc118968247)

[3. Meta-skills 11](#_Toc118968248)

[4. Methods of assessment 12](#_Toc118968249)

# 1. Purpose and use

This document (version 2) is an updated appendix to the Overarching Assessment Strategy for competence-based qualifications. This sets out the requirements that are specific to assessment of the qualifications specified and covers the arrangements for the use of simulation and guidance on unit assessment for the Diploma in Digital Technology at SCQF Level 6 and 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 qualifications.

The Diploma in Digital Technology at SCQF Level 6 is designed to recognise the competence of junior professional digital technology practitioners. The Diploma in Digital Technology at SCQF Level 8 is designed to recognise the competence of associate professional digital technology practitioners. Both qualifications require that the learner is employed in a relevant digital technology role and that workplace learning is aligned to, and assessed against, the performance requirements, knowledge and understanding requirements, and the meta-skills set out. Workplace learning is a partnership between learner, employer and learning provider and all learners must have the support of an employer in undertaking these qualifications.

There are five pathway options that are available as part of the Diploma in Digital Technology at SCQF Level 6 qualification. These are as follows:

* Diploma in Digital Technology: Data Analytics at SCQF Level 6
* Diploma in Digital Technology: Cyber Security at SCQF Level 6
* Diploma in Digital Technology: Software Development at SCQF Level 6
* Diploma in Digital Technology: IT Support at SCQF Level 6
* Diploma in Digital Technology: Infrastructure at SCQF Level 6

There are six 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
* Diploma in Digital Technology: IT Support at SCQF Level 8
* Diploma in Digital Technology: Network Infrastructure at SCQF Level 8
* Diploma in Digital Technology: Cloud Infrastructure 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 Quality assurance requirements

These qualifications are quality assured as set out in the Overarching assessment strategy for competence-based qualifications section 2.

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 qualifications will be delivered and assessed in the workplace. This is the environment in which learners will routinely be engaged in applying digital technologies to support their own organisation in developing and delivering quality products and services through the application of digital technology development skills. These qualifications are designed to recognise competence in the application of digital technologies in different sectoral contexts.

This requires that learners are engaged in a relevant 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 these qualifications.

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

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

There are no further requirements specific to these qualifications.

## 2.2 Occupational expertise and qualification requirements for those assessing or undertaking quality assurance of assessment

The requirements of assessors, internal verifiers and external verifiers are set out in section 2.2 of the Overarching Assessment Strategy for competence-based qualifications. There are no further requirements specific to these qualifications.

## 2.3 Evidence requirements for assessment

Assessment evidence should be generated over a period of time and therefore more than one piece of evidence is expected. For example, this should be ongoing throughout the compilation of a portfolio of evidence. Assessors will need to determine when a candidate has provided enough evidence of sufficient quality to confirm the candidate has reached the required standard.

## 2.4 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 in line with the guidance set out in section 2.1.3 of the Overarching Assessment Strategy. Where simulation is permitted assessment must be conducted in a Realistic Working Environment, under conditions which replicate those of the workplace, and assessors must ensure that competence is fully transferable to the workplace. 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.

**The following tables indicate the units and performance requirements where simulation is permitted:**

**Diploma in Digital Technology at SCQF level 6**

|  |  |  |  |
| --- | --- | --- | --- |
| **Developer Code** | **Unit Title** | **Mandatory/optional /additional** | **Permissible for simulation and rationale** |
| **Mandatory common units** |
| SDS261 | Applying problem solving approaches | Mandatory | Not permissible for simulation |
| SDS262 | Producing documentation to support organisational process delivery  | Mandatory | Not permissible for simulation |
| SDS263 | Defining requirements to support project delivery | Mandatory | Not permissible for simulation |
| US0194 | Development meta-skills and personal practice  | Mandatory | Not permissible for simulation |
| **Data analytics pathway units** |
| SDS251 | Contributing to data management​ | Mandatory | Performance requirements 3 and 5. Managing data may be problematic in a live production environment. This could be equally simulated offline to provide a realistic and safe environment for sourcing, extracting, and sharing data and entering data. |
| SDS252 | Contributing to data manipulation | Mandatory | Performance requirements 2-6. Manipulating data is an offline activity, but may be exposed to sensitive or confidential information, so alternative simulated data sets could be used that present the same rigour and evidence of competence in a safe environment. |
| SDS253 | Contributing to data visualisation and reporting​ | Mandatory | Performance requirements 1-5. Data visualisation and reporting are offline activities, and can be subject to sensitive or confidential information, so alternative simulated data sets could be used for visualisation that present the same rigour and evidence of competence in a safe environment. |
| SDS250 | Contributing to data analysis | Mandatory | Performance requirements 1-4. Analysing data is an offline activity, and can be subject to sensitive or confidential information, so alternative simulated data sets could be used for analysis that present the same rigour and evidence of competence in a safe environment. |
| **Cyber security pathway units** |
| SDS248 | Supporting cyber security governance ​ | Mandatory | Not permissible for simulation |
| SDS247 | Contributing to the implementation of cyber security controls​ | Mandatory | Performance requirements 1-4. Security controls include technical implementations including operating system and application patching, firewall and anti-malware implementation in live systems. It will not always be practical to implement controls 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. |
| SDS246 | Contributing to cyber security risk assessment and management | Mandatory | Not permissible for simulation |
| SDS244 | Contributing to cyber security awareness programmes | Mandatory | Not permissible for simulation |
| SDS245 | Contributing to network vulnerability analysis | Optional  | Performance requirements 2, 4 and 5. Security vulnerability testing involves scanning live environments to identify vulnerabilities in organisation’s network systems and applications. It is accepted practice to develop competency in vulnerability analysis through deploying a range of vulnerabilities into simulated environments where they can be detected. This is not practical in live environments. |
| SDS249 | Supporting cyber security incident response and management | Optional  | Performance requirements 1, 3 and 4. 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. |
| **Software development pathway units** |
| SDS242 | Supporting software design | Mandatory | Not permissible for simulation |
| SDS240 | Contributing to implementing software development methodologies | Mandatory | Not permissible for simulation |
| SDS243 | Supporting software solution development | Mandatory | Not permissible for simulation |
| SDS241 | Providing support for deployed software solutions) | Mandatory | Not permissible for simulation |
| SDS239 | Contributing to deploying software solutions | Mandatory | Not permissible for simulation |
| **IT support pathway units** |
| SDS256 | Supporting digital technology service requests | Mandatory | Performance requirements 1, 3 and 5. Accessing live service requests may be problematic in a live production environment. These could be equally simulated offline to provide a realistic and safe environment for responding to them. |
| SDS254 | Assisting development of digital technology support materials | Mandatory | Not permissible for simulation |
| SDS255 | Supporting digital technology asset management | Mandatory | Performance requirements 1-3. Accessing live asset scenarios may be problematic for some support analysts in a live production environment. These could be equally simulated offline to provide a realistic and safe environment for monitoring and recording assets and installing software licenses. |
| **IT infrastructure pathway units** |
| SDS259 | Contributing to implementing on-premises physical network infrastructure | Mandatory | Performance requirements 1-5. Implementing network infrastructure involves creating live network environments and testing them and so from a learning perspective undertaking off-line network implementation in simulated environments would provide the same rigour and evidence of competence in a controlled environment. |
| SDS258 | Contributing to configuring and maintaining cloud infrastructure | Mandatory | Performance requirements 1-6. Accessing live cloud environments may be problematic in a live production environment. These could be equally simulated offline or using test environments to provide a realistic and safe environment for configuring and maintaining cloud infrastructure. |
| SDS257 | Assisting with implementing wireless network infrastructure  | Optional  | Performance requirements 2-6 and 6. Accessing wireless network environments may be problematic in a live production environment. These could be equally simulated offline or using test environments to provide a realistic and safe environment for implementing wireless network infrastructure. |
| SDS260 | Supporting cloud migration | Optional  | Performance requirements 2-6. Migrating to live cloud environments may be problematic in a live production environment. These could be equally simulated offline or using test environments to provide a realistic and safe environment for cloud migration. |

*Table 1 – Guidance on the use of simulation for Diploma in Digital Technology for SCQF level 6 units*

**Diploma in Digital Technology at SCQF level 8**

|  |  |  |  |
| --- | --- | --- | --- |
| **Developer Code** | **Unit Title** | **Mandatory/optional /additional** | **Permissible for simulation and rationale** |
| **Mandatory common units** |
| 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 |
| **Data analytics pathway units** |
| 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 | Performance requirements 2-4 and 9. 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 | Performance requirements 1-7. Transforming data is an offline activity, but may be exposed to sensitive or confidential 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 | Performance criteria 1-5. Analysing data is an offline activity, and can be subject to sensitive or confidential 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 | Performance criteria 3-4. Visualising data is an offline activity, and can be subject to sensitive or confidential 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 | Performance criteria 1-10. 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 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.  |
| **Cyber security pathway units** |
| SDS 029 | Contributing to cyber security risk assessment and risk management | Mandatory | Not permissible for simulation |
| SDS 014 | Contributing to intrusion detection activities | Mandatory | Performance criteria 1-7. 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 | Performance criteria 1-8. 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 | Performance criteria 2-6. Security audit and compliance checking involves performing checks on live systems that can involve access to sensitive data and processes. Therefore, it is possible to develop competency in audit and compliance using simulated environments. |
| SDS 017 | Delivering threat intelligence | Optional  | Not permissible for simulation |
| SDS 015 | Contributing to scoping and implementing security testing | Optional  | Performance criteria 1-6. 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  | Performance criteria 3-8. 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  | Performance criteria 3-8. 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. |
| **Software development pathway units** |
| 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 |
| **IT support pathway units** |
| SDS264 | Responding to digital technology service requests | Mandatory | Performance criteria 1-5. Accessing live service requests may be problematic in a live production environment. These could be equally simulated offline to provide a realistic and safe environment for responding to them. |
| SDS265 | Maintaining service support procedures | Mandatory | Not permissible for simulation |
| SDS268 | Providing digital technology asset management | Mandatory | Not permissible for simulation |
| SDS266 | Producing and testing automation scripts | Mandatory | Not permissible for simulation |
| SDS267 | Producing service management reports and metrics | Mandatory | Not permissible for simulation |
| **Network infrastructure pathway units** |
| SDS269 | Designing and implementing network systems | Mandatory | Performance criteria 1-7. Designing and implementing network systems involves creating live network environments and testing them and so from a learning perspective undertaking off-line network design and implementation in simulated environments would provide the same rigour and evidence of competence in a controlled environment. |
| SDS270 | Implementing network security | Mandatory | Performance criteria 2-3 and 5-8. Implementing network security involves installing security devices, evaluating network security compliance, monitoring network traffic, and reviewing network audit logs for security issues. It will not always be practical to implement network security devices into live environments as this could risk their normal operation, and so the potential of undertaking network security implementation and testing in simulated environments would provide the same rigour and evidence of competence in a controlled environment. |
| **Cloud infrastructure pathway units** |
| SDS271 | Creating and deploying cloud applications | Mandatory | Performance criteria 1-7. Accessing live cloud environments may be problematic in a live production environment. These could be equally simulated offline or using test environments to provide a realistic and safe environment for creating and deploying cloud applications. |
| SDS272 | Implementing cloud security | Mandatory | Performance criteria 1-8. Implementing cloud security involves implementing cloud environment hardening, data encryption, access management, and intrusion detection and prevention technology. It also includes conducting security assessments and identifying and resolving cloud security issues. It is not practical to implement cloud security in live environments as this could risk their normal operation, and so the potential of undertaking cloud security implementation and testing in simulated environments would provide the same rigour and evidence of competence in a controlled environment. |

*Table 2 – Guidance on the use of simulation for Diploma in Digital Technology for SCQF level 8 units*

# 3. Meta-skills

A key aspect of the digital technology qualifications 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 practice is included in the Digital Technology qualification at SCQF level 6. This specifically requires learners to be able to achieve the following learning outcome:

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

The unit Developing meta-skills and personal professionalism is included in the Digital Technology qualification at SCQF level 8. This 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.

It is intended that the assessment of these units will draw holistically on the assessment and evidence from the other units within the qualifications as learners carry out their normal day to day work activities, solve problems and work with others to achieve their objectives.

The process of self-assessment, reflection and evaluation of practice are central to the development of an individual’s job specific skills and their meta-skills. This involves learners taking ownership of their learning by reviewing their work and reflecting on their progress. Accordingly, most organisational performance management processes involve setting clear objectives, agreeing development activities and conducting regular progress reviews and feedback. This enables evidence of the development of individuals’ job specific skills and meta-skills to be generated naturally as part of the performance management process.

In summary, the meta-skills unit is integrated with the other units of the qualification rather than being viewed as a standalone unit. The associated performance requirements and knowledge and understanding requirements are generated through the other units and assessed through the performance management process.

Furthermore, assessment of the meta-skills should focus on the nature and quality of the self-reflective practices and self-evaluation activities being undertaken, rather than the achievement 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.

Section 3 of the Overarching Assessment Strategy provides guidance on the assessment of meta-skills to be used in conjunction with this assessment strategy appendix. The tools and approaches referred to in the Overarching Assessment Strategy are for guidance, therefore flexible approaches may be used to ensure assessment is relevant to individuals working in different organisations. 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.

# 4. Methods of assessment

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

A range of assessment methods have been identified during the design of the digital technology qualifications at SCQF level 6 and SCQF level 8. Learners are expected to provide evidence of meeting all the knowledge and understanding and performance requirements 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 the digital technology qualifications.



 *Table 3 – Assessment methods identified to support the pathways in the Diploma in Digital Technology at SCQF level 6*



 *Table 4 – Assessment methods identified to support the pathways in the Diploma in Digital Technology at SCQF level 8*

It is recommended that learners undertaking the Diploma in Digital Technology at SCQF Level 6 and the Diploma in Digital Technology at SCQF Level 8 develop a portfolio of work to evidence their competence. The portfolio may contain a variety of different types of evidence, collected over time. This approach will allow learners to collect evidence of achievement in ways that are most appropriate to their job role as well as the qualification being undertaken.

Knowledge and understanding can be demonstrated in several different ways, but it is suggested that the most appropriate methods for these qualifications are case studies, professional discussion and presentation. Assessors should ensure they ask relevant questions that reflect the content of the unit being assessed and enable learners to demonstrate knowledge and understanding as defined within the unit.