Level 5 Award in Industrial Cyber Security – Detect, Respond, Recover

Qualification Handbook

Qualification Number: 610/7118/3

Qualifications Wales Number: C00/5363/0

Operational Start Date: 1st March 2026

The Workforce Development Trust

Skills for Justice

Skills for Health

SFJ Awards

People 1st International

iCQ Awards

Contents

Document Control

Revisions and Amendment Register

Date of Issue	Page No	Revision	Version
March 2026			1

1. Introduction

1.1. About SFJ Awards

SFJ Awards is part of the Workforce Development Trust group, together with Skills for Justice, Skills for Health and People 1st International. The Workforce Development Trust is a not-for-profit organisation helping employers to continually improve their workforce through increasing productivity, improving learning solutions and helping to boost the skills for staff across a wide range of industries throughout the UK and internationally.

SFJ Awards is an independent Awarding Organisation, regulated by the UK qualifications regulators, including Ofqual, CCEA and Qualifications Wales, to assess, quality assure and certificate learners and employees, helping training providers and employers to continue developing a highly skilled workforce for the future. Our values are 'For Skills, For Flexibility and For Jobs' and our work embodies the core charitable aims of the wider Workforce Development Trust group that ultimately supports better jobs. We add value to employers and training providers by delivering a wide range of sector-specific regulated qualifications, bespoke learner certification and quality assurance; SFJ Awards is also an Apprenticeship Organisation for Apprenticeships in England.

Whilst predominantly delivering qualifications and assessments to meet the needs of Policing, Fire and Rescue, Community Justice, Custodial Care, Armed Forces, Security and Emergency Services, we continue to grow into markets that require a robust, and quality assured certification solution.

1.2. Customer Service Statement

Our Customer Service Statement is published on the SFJ Awards website giving the minimum level of service that centres can expect. The Statement will be reviewed annually and revised as necessary in response to customer feedback, changes in legislation, and guidance from the qualifications regulators.

1.3. Centre Support

SFJ Awards works in partnership with its customers. For help or advice contact:

Tel: 0114 284 1970

SFJ Awards
Consult House
Meadowcourt Business Park
4 Hayland Street
Sheffield
S9 1BY

Email: info@sfjawards.com
Website: www.sfjawards.com

2. The Qualification

2.1. Qualification Objective

The objective of the **Level 5 Award in Industrial Cyber Security – Detect, Respond, Recover** is to equip learners with the advanced knowledge and applied skills required to effectively manage cyber incidents within industrial and Critical National Infrastructure environments.

The qualification is designed to enable learners to detect complex cyber threats, respond appropriately to cyber incidents while maintaining operational safety and continuity, and recover systems and services following an attack. It supports the development of professional judgement, technical competence, and incident-management capability across the full cyber-incident lifecycle, strengthening organisational resilience and readiness in safety-critical and regulated contexts.

2.2. Pre-entry Requirements

There are no pre-entry requirements for this qualification. However centres must ensure that learners are able to complete this qualification, for example, through completing a skills scan to ensure they can work at the appropriate level.

2.3. Qualification Structure

To be awarded this qualification the learner must achieve **3** mandatory units as shown in the table below.

Mandatory Units					
Unit Number	**Odyssey Reference**	**Unit Title**	**Level**	**GLH**	**TuT**
1	6855	Detecting Complex Cyber Threats to Critical National Infrastructure	5	30	37
2	6856	Responding to Complex Cyber Threats Within Critical National Infrastructure	5	22	24
3	6857	Recovering from Complex Cyber Incidents Within Critical National Infrastructure	5	12	14

2.4. Total Qualification Time (TQT)

Values for Total Qualification Time[1], including Guided Learning, are calculated by considering the different activities that Learners would typically complete to achieve and demonstrate the learning outcomes of a qualification. They do not include activities which are required by a Learner's Teacher based on the requirements of an individual Learner and/or cohort. Individual Learners' requirements and individual teaching styles mean there will be variation in the actual time taken to complete a qualification. Values for Total Qualification Time, including Guided Learning, are estimates.

Some examples of activities which can contribute to Total Qualification Time include:

- Independent and unsupervised research/learning
- Unsupervised compilation of a portfolio of work experience
- Unsupervised e-learning
- Unsupervised e-assessment
- Unsupervised coursework
- Watching a pre-recorded podcast or webinar
- Unsupervised work-based learning
- All Guided Learning

[1] Total Qualification Time, Ofqual
https://www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

Some examples of activities which can contribute to Guided Learning include:

- Classroom-based learning supervised by a Teacher
- Work-based learning supervised by a Teacher
- Live webinar or telephone tutorial with a Teacher in real time
- E-learning supervised by a Teacher in real time
- All forms of assessment which take place under the Immediate Guidance or Supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training, including where the assessment is competence-based and may be turned into a learning opportunity.

The Total Qualification Time and Guided Learning Hours for this qualification are as follows:

Qualification Title	TQT	GLH
SFJ Awards Level 5 Award in Industrial Cyber Security – Detect, Respond, Recover	75	64

2.5. Grading

This qualification is graded pass / fail.

2.6. Age Range and Geographical Coverage

This qualification is recommended to learners aged **18** years and over and is regulated in England and Wales.

2.7. Opportunities for Progression

The Level 5 Award in Industrial Cyber Security – Detect, Respond, Recover supports progression into senior operational and technical roles within cyber security and Critical National Infrastructure (CNI) environments. It is particularly suited to professionals seeking to develop or formalise their expertise in OT/IT security, incident response, and organisational cyber resilience.

Learners may progress into roles such as Cyber Security Analyst (OT/ICS), Incident Response Lead, Cyber Resilience Manager, or other specialist positions responsible for safeguarding operational technology and critical services.

The qualification also provides a foundation for further study at Level 6 or above in cyber security, digital forensics, cyber resilience, or related technical and security disciplines.

2.8. Use of Languages

SFJ Awards business language is English and we provide assessment materials and qualification specifications that are expressed in English. Assessment specifications and assessment materials may be requested in Welsh or Irish and, where possible, SFJ Awards will try to fulfil such requests. SFJ Awards will provide assessment materials and qualification specifications that are expressed in Welsh or Irish and support the assessment of those learners, where the number of learners makes it economically viable for SFJ Awards to do so. More information is provided in the SFJ Awards' Use of Language Policy.

For learners seeking to take a qualification and be assessed in British Sign Language or Irish Sign Language, please refer to SFJ Awards' Reasonable Adjustments Policy. A learner may be assessed in British Sign Language or Irish Sign Language where it is permitted by SFJ Awards for the purpose of Reasonable Adjustment.

Policies are available on our website sfjawards.com or on request from SFJ Awards.

3. Qualification Units

3.1. Mandatory Units

Title	Detecting Complex Cyber Threats to Critical National Infrastructure
Level	5
Unit Number	1
GLH	30

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand complex threat actors, attack methodologies and indicators of compromise within Critical National Infrastructure (CNI)	1.1	Evaluate a range of threat actors and the likely impact of cyber-attacks against the relevant CNI	Could include: • State-sponsored, criminal, insider and hacktivist threat groups • CNI-specific attacker motivations: disruption, sabotage, espionage • Multi-vector attacks (cyber–physical, social engineering)

			• Real-world CNI case studies (e.g., Triton/Trisis, Ukraine grid) • Impacts on safety, operations, environment, reputation and regulation • NIS2-aligned threat categories and sector-specific risks
	1.2	Analyse techniques and tools used by known cyber threat groups, and their impact on detection and defence strategies	Could include: • MITRE ATT&CK for ICS/OT • Exploitation of industrial protocols (Modbus, OPC-UA, DNP3) • Supply-chain compromise and vendor access abuse • Living-off-the-land techniques in OT • Firmware manipulation, logic injection, remote command exploitation

			• How attacker tooling bypasses traditional detection
	1.3	Critically analyse digital forensic evidence to identify indicators of compromise and actor behaviours	Could include: • Forensic artefacts: logs, historian data, PLC changes, captures • Identifying modified logic, suppressed alarms, rogue commands • Time-series and event timeline reconstruction • Actor behaviours reflected in artefacts (pivoting, persistence) • OT-safe forensic techniques (non-disruptive acquisition)
	1.4	Evaluate how digital forensic findings inform detection, response, and recovery strategies	Could include: • Using forensic outcomes to refine SIEM / ICS detection

			• Linking evidence to containment priorities • Informing engineering change control and safety case revisions • Improving recovery verification steps • Use of kill-chain mapping to support strategic defence
2. Understand technical systems and vulnerabilities relevant to threat detection	2.1	Critically evaluate technical controls including: • network segmentation • trusted device utilisation • detection techniques • backup processes	
	2.2	Evaluate the factors and evidence used to distinguish between operational faults and potential cyber incidents	For example; • Baseline deviation analysis • Using safety-system logs vs cyber logs to validate anomalies

			• Distinguishing mechanical/electrical faults from malicious commands • Digital twin or simulation comparison • Correlating alerts, operator actions and system states
	2.3	Evaluate the purpose and limitations of a range of Operational Technology (OT) systems	Consider their contribution to operational continuity and cyber security
	2.4	Analyse the potential operational, safety and security consequences arising from the misuse or compromise of Operational Technology (OT) systems	For example: • Unsafe states: overspeed, overpressure, temperature runaway • Cascading failures across interdependent CNI systems • Service disruption (black start, contamination, transport outages)

			• Physical damage scenarios (pumps, turbines, chemical valves)
	2.5	Describe the interaction between Operational Technology (OT) and Information Technology (IT) systems and its implications for cyber security within CNI environments	For example; • Converged authentication (AD for ICS) • Data flow across IT–OT boundaries • Remote vendor access channels • Shadow OT and unmanaged devices • Attack paths from IT → OT
3. Be able to apply detection tools and techniques within a Critical National Infrastructure (CNI) environment	3.1	Use appropriate tools to identify indicators of compromise within Operational Technology (OT) systems	For example: • ICS-aware monitoring tools (conceptual vendor-neutral) • Passive network monitoring & safe packet capture • Signature vs anomaly-based detection methods

			• OT-specific IOC identification • Event correlation and alert validation
	3.2	Demonstrate the secure and effective operational use of a trusted device in accordance with organisational security protocols	
Additional information about the unit			
Assessment guidance	This unit is assessed through a portfolio of evidence. Learners must demonstrate both critical understanding of complex cyber threats within Critical National Infrastructure (CNI) environments and the practical application of detection tools and techniques within an Operational Technology (OT) context. Evidence should reflect analytical depth and professional judgement appropriate to Level 5. Written reports, case study analysis, technical evaluations, and reflective accounts should demonstrate the learner's ability to evaluate threat actors, analyse attack methodologies, interpret digital forensic evidence, and assess the effectiveness and limitations of technical controls within CNI settings. Responses must move beyond description and show reasoned evaluation, consideration of safety and operational impact, and awareness of the interaction between IT and OT systems. Practical competence must also be evidenced. Learners should demonstrate the safe and secure use of detection tools and trusted devices in line with organisational protocols. Evidence may include observation records, system outputs, logs, or authenticated workplace		

	documentation. Where access to live environments is not appropriate, robust simulation may be used, provided it reflects the constraints and safety requirements of CNI operations. All evidence must comply with organisational security, confidentiality, and safety requirements. Assessors must ensure the portfolio demonstrates authentic, sufficient, and clearly attributable evidence of both analytical capability and applied technical skill within complex, safety-critical environments.

Title	Responding to Complex Cyber Threats to Critical National Infrastructure
Level	5
Unit Number	2
GLH	22

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand the incident response process within Critical National Infrastructure (CNI)	1.1	Explain how to locate and action cyber incident response procedures	Could include: • Accessing IR playbooks and escalation trees • Interpreting severity levels and activation criteria • Out-of-band communication methods • IR documentation for regulator scrutiny
	1.2	Evaluate the factors influencing the selection and implementation of appropriate incident response protocols	For example; • Safety implications vs containment urgency

			• Impact on operational continuity and critical services • Regulatory reporting triggers (NIS2/CAF) • Multi-site and multi-system coordination • Vendor and third-party involvement constraints
	1.3	Evaluate the roles and interdependencies of individuals and teams involved in incident response, and the importance of effective collaboration	Could include: • SOC, OT engineers, operations control rooms, management • Physical-security interface during cyber events • External collaboration: regulators, law enforcement, vendors • Communication pitfalls and escalation timing
	1.4	Critically assess organisational approaches to responding to cyber incidents	For example;

			• IR maturity evaluations (CAF, NIST) • Effectiveness of rehearsals and tests • Capability gaps (resourcing, tooling, governance) • Comparison of planned vs actual performance in incidents
	1.5	Assess the implications of misclassification for organisational response and overall resilience	• Underclassification = delayed containment, regulatory breaches • Overclassification = unnecessary shutdown, operational risk • SOC alerting vs OT operational context • Misclassification case studies

	1.6	Evaluate cyber security processes within own area of CNI in relation to prevention and mitigation	• Change control, access control, segmentation processes • Monitoring, patching and backup regimes • Known process gaps and improvement opportunities • Integration with operational safety processes
2. Be able to apply cyber incident response procedures within Critical National Infrastructure (CNI)	2.1	Apply organisational cyber incident response procedures within a specific area of CNI	
	2.2	Demonstrate the process of gathering and documenting incident information to support organisational response activities	
	2.3	Demonstrate effective communication and coordination with relevant internal and external stakeholders during an incident response scenario	
	2.4	Implement containment actions in line with organisational procedures and operational safety requirements	

Additional information about the unit	
Assessment guidance	This unit is assessed through a portfolio of evidence. Learners must demonstrate both a critical understanding of incident response processes within Critical National Infrastructure (CNI) environments and the ability to apply those processes effectively in practice. Portfolio evidence should demonstrate analytical depth appropriate to Level 5. Written evaluations, case study analysis, professional discussions, and reflective accounts should show the learner's ability to assess incident response procedures, evaluate organisational approaches, and consider the operational, regulatory, and safety implications of response decisions. Evidence should demonstrate understanding of the roles and interdependencies within incident response teams and the impact of decision-making on organisational resilience. Learners must also evidence practical application. This should include applying organisational incident response procedures within a defined CNI context, documenting incident information accurately, communicating effectively with relevant stakeholders, and implementing containment actions in line with safety and operational requirements. Evidence may include observation records, incident documentation, logs, meeting notes, authenticated workplace records, or robust simulation outputs. Where simulation is used, it must reflect realistic CNI constraints, including safety-critical considerations and multi-stakeholder coordination. All assessment activity must comply with organisational security, confidentiality, and regulatory requirements.

Title	Recovering From Cyber Incidents Within Critical National Infrastructure
Level	5
Unit Number	3
GLH	12

Learning Outcomes *The learner will:*	**Assessment Criteria** *The learner can:*		**Guidance and/or Indicative Content**
1. Understand post-incident recovery and improvement processes	1.1	Explain the value of effective testing and exercising of incident response and post-incident recovery procedures	
	1.2	Evaluate individual responsibilities and required actions during the post-incident recovery process	
	1.3	Explain the importance of lessons identified and lessons learned in supporting continuous improvement	
	1.4	Evaluate appropriate controls and mitigations to minimise the impact and recurrence of future events	• Hardening improvements (segmentation, access, logging)

			• OT system security baselining and configuration integrity • Engineering change control enhancements • Monitoring expansion and visibility improvements • Prioritising mitigations via risk and cost-benefit analysis
	1.5	Explain the regulatory and legal frameworks governing post-incident reporting, recovery and improvement requirements within CNI	Explain regulatory and legal frameworks governing the prevention and mitigation of cyber incidents within CNI
2. Be able to apply organisational recovery and improvement procedures within Critical National Infrastructure (CNI)	2.1	Analyse recovery activities to detect lessons identified and lessons learned, distinguishing between immediate observations and validated learning	For example: • RCA methods (5 Whys, fishbone, bow-tie) • Identifying systemic vs localised lessons • Prioritising learning actions

	2.2	Produce structured lessons learned documentation that supports organisational learning and continuous improvement	For example: • Producing structured lessons-learned reports • Linking lessons to future preventative actions • Communicating learning across engineering, operations and cyber teams
	2.3	Demonstrate the secure and safe operation of relevant Operational Technology (OT) systems in line with organisational procedures and regulatory requirements	For example: • Operating within safe modes following compromise • Performing functional validation checks • Documenting recommissioning activity • Ensuring compliance with sector safety regulations
	2.4	Apply organisational recovery and restoration procedures to return systems or services to operational status following a cyber incident	For example:

			• Restoring backups and verifying baseline configurations. • Rebuilding compromised devices or workstations. • Validating system performance before full operation. • Completing regulatory or audit documentation.
Additional information about the unit			
Assessment guidance	This unit is assessed through a portfolio of evidence. Learners must demonstrate both a critical understanding of post-incident recovery and improvement processes and the ability to apply organisational recovery procedures within a Critical National Infrastructure (CNI) context. Portfolio evidence should demonstrate evaluative and analytical thinking appropriate to Level 5. Written assignments, case study analysis, professional discussions, and reflective accounts should show the learner's ability to assess recovery strategies, evaluate responsibilities during post-incident activity, and consider the regulatory and legal frameworks governing recovery and reporting within CNI environments. Evidence must move beyond description and demonstrate reasoned judgement, particularly in relation to risk reduction, resilience improvement, and prevention of recurrence. Practical application must also be evidenced. Learners should demonstrate their ability to analyse recovery activity to identify lessons identified and lessons learned, produce structured		

	documentation that supports organisational learning, and apply recovery and restoration procedures safely and securely. Evidence may include observation records, authenticated workplace documentation, recovery reports, lessons learned documentation, system validation records, or outputs from robust simulation. Where simulation is used, it must reflect realistic CNI constraints, including operational continuity, safety requirements, and regulatory considerations. All assessment activity must comply with organisational security, safety, and confidentiality requirements.

4. Centre Requirements

4.1. Centre Responsibilities

Centres must be approved by SFJ Awards and also have approval to deliver the qualifications they wish to offer. This is to ensure centres have the processes and resources in place to deliver the qualifications. Approved centres must adhere to the requirements detailed in the SFJ Awards Centre Handbook, which includes information for centres on assessment and internal quality assurance processes and procedures.

When a centre applies to offer a qualification, they will need to provide evidence that they have sufficient resources and infrastructure in place for delivery of that qualification:

- evidence of assessor and IQA competence
- sample assessment materials and mark schemes
- scheme of work
- details of available resources.

Centres are responsible for ensuring that their assessor and internal quality assurance staff:

- are occupationally competent and/or knowledgeable as appropriate to the assessor or IQA role they are carrying out
- have current experience of assessing/internal quality assuring as appropriate to the assessor or IQA role they are carrying out
- have access to appropriate training and support
- are independent and any conflicts of interests are managed and monitored appropriately by SFJ Awards.

Information on the induction and continuing professional development of those carrying out assessment and internal quality assurance must be made available by centres to SFJ Awards through the external quality assurance process.

This handbook should be used in conjunction with the following SFJ Awards documents:

- Assessment Guidance
- Centre Handbook
- Centre Assessment Standards Scrutiny (CASS) Strategy
- Conflict of Interest Policy
- Whistleblowing Policy
- Malpractice and Maladministration Policies

- Equality and Diversity Policy
- Appeals Policy
- Complaints Policy
- Sanctions Policy
- Examinations and Invigilation Policy
- Risk and Centre Monitoring Policy
- Fair Access and Equality of Opportunity Policy
- Reasonable Adjustment and Special Considerations Policy
- Standardisation Policy
- Direct Claims Policy
- Centre Approval Process

All documents referenced in the strategy are available to centres on Odyssey, SFJ Awards learner management system, or on request from SFJ Awards.

4.2. Centre Assessment Standards Scrutiny (CASS) Strategy

Centres are **permitted** to develop and mark assessments for the qualification(s) in this handbook, in line with our CASS Strategy.

4.3. Facilities

Training and assessment for approved qualifications must take place in a suitable environment that has been approved by SFJ Awards. The environment must be adequately equipped for training, conducive to effective learning, and must comply with current Health and Safety requirements. Equipment for practical activities must be readily available and fit for purpose. All examination venues must comply with the policy, standards, and regulations specified by SFJ Awards to gain approval for knowledge-based assessment.

Training and assessment facilities must comply with the ongoing approval arrangements of SFJ Awards.

4.4. Trainers

Some sectors specify trainer requirements for qualification delivery, for example first aid and security. Details of any specific trainer requirements are included in this qualification handbook. Centres should therefore check the handbook, or with SFJ Awards, for any trainer requirements that apply to the qualification(s) they wish to deliver. Centres applying for approval with SFJ Awards will be required to provide SFJ Awards with current evidence of how each trainer meets the requirements, for example certificates of achievement, CV or CPD records.

5. Assessment

5.1. Qualification Assessment Methods

Assessment methods[2] that can be used for the SFJ Awards Level 5 Award in Industrial Cyber Security – Detect, Respond, Recover are as follows:

- Aural Examination
- E-assessment
- Portfolio of Evidence (including for example records of professional discussions, question and answer sessions, work products)
- Practical Demonstration / Assignment
- Practical Examination
- Task-based Controlled Assessment
- Written Examination
- Observation
- Professional Discussion
- Interview
- Presentation and Questioning
- Project

5.2. Assessing Competence

The purpose of assessing competence is to make sure that an individual is competent to carry out the activities required in their work.

Assessors gather and judge evidence during normal work activities to determine whether the learner demonstrates their competence against the standards in the qualification units. Competence should be demonstrated at a level appropriate to the qualification. The skills required at the different qualification levels are defined in Ofqual's level descriptors.[3] Further information on qualification levels is included in the SFJ Awards Assessment Guidance.

Evidence must be:

- Valid
- Authentic
- Sufficient
- Current

[2] Selected from assessment methods listed on Ofqual's regulatory system (Portal)
[3] Ofqual Handbook: General Conditions of Recognition, Section E - Design and development of qualifications www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

- Reliable

Assessment should be integrated into everyday work to make the most of opportunities that arise naturally within the workplace.

5.3. Methods for Assessing Competence

Qualifications may be assessed using any method, or combination of methods, as stipulated either by SFJ Awards or within specific qualifications, and which clearly demonstrate that the learning outcomes and assessment criteria have been met. Some sectors may have specific assessment requirements that apply to their qualifications and where these apply, details will be included in the qualification-specific handbook.

Assessors need to be able to select the right assessment methods for the competences that are being assessed, without overburdening the learner or the assessment process, or interfering with everyday work activities. SFJ Awards expect assessors to use a combination of different assessment methods to make a decision about an individual's occupational competence. Assessment methods which are most likely to be used are outlined below. However, these are included for guidance only and there may be other methods which are suitable. Further information on assessment methods is included in the SFJ Awards Assessment Guidance.

5.3.1. Observation

SFJ Awards believe that direct observation in the workplace by an assessor or testimony from an expert witness is preferable as it allows for authenticated, valid and reliable evidence. Where learners demonstrate their competence in a real work situation, this must be done without the intervention from a tutor, supervisor or colleague.

However, SFJ Awards recognise that alternative sources of evidence and assessment methods may have to be used where direct observation is not possible or practical.

5.3.2. Testimony of Witnesses and Expert Witnesses

Witness testimonies are an accepted form of evidence by learners when compiling portfolios. Witness testimonies can be generated by peers, line managers and other individuals working closely with the learner. Witnesses are defined as being those people who are occupationally expert in their role.

Testimony can also be provided by expert witnesses who are occupationally competent **and** familiar with the qualification units. Assessors will not need to spend as long assessing expert witness testimony as they would a witness testimony from

a non-expert. Therefore, if expert witnesses are involved in the assessment strategy for a qualification a greater number of learners can be managed by a smaller number of assessors.

The assessor is however responsible for making the final judgement in terms of the learner meeting the evidence requirements for the qualification units.

5.3.3. Work Outputs (Product Evidence)

Examples of work outputs include plans, reports, budgets, photographs, videos or notes of an event. Assessors can use work outputs in conjunction with other assessment methods, such as observation and discussion, to confirm competence and assure authenticity of the evidence presented.

5.3.4. Professional Discussion

Discussions allow the learner to describe and reflect on their performance and knowledge in relation to the standards. Assessors can use discussions to test the authenticity, validity and reliability of a learner's evidence. Written/audio records of discussions must be maintained.

5.3.5. Questioning the Learner

Questioning can be carried out orally or in written form and used to cover any gaps in assessment or corroborate other forms of evidence. Written/audio records of all questioning must be maintained.

5.3.6. Simulations

Simulations may take place in a non-operational environment which is not the learner's workplace, for example a training centre. The assessment guidance attached to each unit in section 3 of the handbook will specify where simulations are authorised. Please note that proposed simulations **must** be reviewed to ensure they are fit for purpose as part of the IQA's pre-delivery activity.

Simulations can be used when:

- the employer or assessor consider that evidence in the workplace will not be demonstrated within a reasonable timeframe
- there are limited opportunities to demonstrate competence in the workplace against all the assessment criteria

- there are health and safety implications due to the high-risk nature of the work activity
- the work activity is non-routine and assessment cannot easily be planned for
- assessment is required in more difficult circumstances than is likely to happen day to day.

Simulations must follow the principles below:

1. The nature of the contingency and the physical environment for the simulation must be realistic
2. Learners should be given no indication as to exactly what contingencies they may come across in the simulation
3. The demands on the learner during the simulation should be no more or less than they would be in a real work situation
4. Simulations must be planned, developed and documented by the centre in a way that ensures the simulation correctly reflects what the specific qualification unit seeks to assess and all simulations should follow these documented plans
5. There should be a range of simulations to cover the same aspect of a unit and they should be rotated regularly.

5.4. Assessing Knowledge and Understanding

Knowledge-based assessment involves establishing what the learner knows or understands at a level appropriate to the qualification. The depth and breadth of knowledge required at the different qualification levels are defined in Ofqual's level descriptors.[4] Further information on qualification levels is included in the SFJ Awards Assessment Guidance.

Assessments must be:

- Fair
- Robust
- Rigorous
- Authentic
- Sufficient
- Transparent
- Appropriate

[4] Ofqual Handbook: General Conditions of Recognition, Section E - Design and development of qualifications www.gov.uk/guidance/ofqual-handbook/section-e-design-and-development-of-qualifications

Good practice when assessing knowledge includes use of a combination of assessment methods to ensure that as well as being able to recall information, the learner has a broader understanding of its application in the workplace. This ensures that qualifications are a valid measure of a learner's knowledge and understanding.

A proportion of any summative assessment may be conducted in controlled environments to ensure conditions are the same for all learners. This could include use of:

- Closed book conditions, where learners are not allowed access to reference materials
- Time bound conditions
- Invigilation.

Where assessment in controlled environments is considered appropriate for qualifications, or the use of specific assessment materials (for example, exemplars or scenarios) is required, information will be included in the qualification handbook.

5.5. Methods for Assessing Knowledge and Understanding

SFJ Awards expect assessors to use a variety of different assessment methods to make a decision about an individual's knowledge and understanding, which are likely to include a combination of the following:

a. Written tests in a controlled environment
b. Evidenced question and answer sessions with assessors
c. Evidenced professional discussions
d. Written assignments (including scenario-based written assignments).

Where written assessments are centre-devised and centre-assessed, centres must:

- maintain a sufficient bank of assignments which are changed regularly
- record how risks in tests/exams conducted in controlled environments are mitigated
- conduct assessments in line with SFJ Awards Examination and Invigilation Policy.

Centres must take into account the qualification when selecting knowledge assessment methods to ensure they are appropriate and allow the learner to evidence the assessment criteria. For example, MCQs are unlikely to be appropriate for higher levels qualifications or assessment criteria which require learners to 'explain', 'describe', 'evaluate' or 'analyse'.

5.6. Assessment Planning

Planning assessment allows a holistic approach to be taken, which focuses on assessment of the learner's work activity as a whole. This means that the assessment:

- reflects the skills requirements of the workplace
- saves time
- streamlines processes
- makes the most of naturally occurring evidence opportunities

Planning assessment enables assessors to track learners' progress and incorporate feedback into the learning process; assessors can therefore be sure that learners have had sufficient opportunity to acquire the skills and knowledge to perform competently and consistently to the standards before being assessed. The assessment is therefore a more efficient, cost effective process which minimises the burden on learners, assessors and employers.

6. Assessor Requirements

6.1. Occupational Knowledge and Competence

Due to the risk-critical nature of the work, particularly when assessing in the public and security sectors, and the legal implications of the assessment process, assessors must understand the nature and context of the learners' work. This means that assessors must be occupationally competent. Each assessor must therefore be, according to current sector practice, competent in the functions covered by the unit(s) they are assessing. They will have gained their occupational competence by working within the sector relating to the unit(s) or qualification(s) they are assessing.

Assessors must be able to demonstrate consistent application of the skills and the current supporting knowledge and understanding in the context of a recent role directly related to the qualification unit(s) they are assessing as a practitioner, trainer or manager.

Where assessors are assessing knowledge-based qualifications, they must be occupationally knowledgeable in the sector they are assessing in.

6.2. Qualification Knowledge

Assessors must be familiar with the qualification unit(s) they are assessing. They must be able to interpret and make judgements on current working practices and technologies within the area of work.

6.3. Assessor Competence

Assessors must be able to make valid, reliable and fair assessment decisions. To demonstrate their competence, we expect assessors to be:

- qualified with a recognised assessor qualification, or
- working towards a recognised assessor qualification.

However, there may be circumstances when assessors have the equivalent competence through training to appropriate national standards, and SFJ Awards will agree this on a case-by-case basis.

Assessors' experience, knowledge and understanding could be verified by a combination of:

- curriculum vitae and employer endorsement or references
- possession of a relevant NVQ/SVQ, or vocationally related qualification
- corporate membership of a relevant professional institution
- interview (the verification process must be recorded and available for audit).

Recognised assessor qualifications include, but are not limited to:

- RQF/QCF Level 3 Award in Assessing Competence in the Work Environment
- RQF/QCF Level 3 Award in Assessing Vocationally Related Achievement
- RQF/QCF Level 3 Certificate in Assessing Vocationally Related Achievement
- An appropriate Assessor qualification in the SCQF as identified by SQA Accreditation
- A1 Assess candidates using a range of methods
- D32/33 Assess candidate performance, using differing sources of evidence.

Where assessors hold an older qualification e.g. D32/33 or A1, they must provide evidence of Continuing Professional Development (CPD) to demonstrate current competence.

Assessors must hold an assessor qualification, or equivalent competence if agreed by SFJ Awards, relevant to the type of qualification(s) they are assessing e.g.

- Level 3 Award in Assessing Competence in the Work Environment:
  For assessors who assess **competence in a work environment**, which requires the use of the following assessment methods: observation, examining work products or outputs, oral questioning, discussion, use of witness testimony, learner statements and Recognition of Prior Learning (RPL).
- Level 3 Award in Assessing Vocationally Related Achievement:

For assessors who assess **knowledge and/or skills in vocationally related areas** using the following assessment methods: tests of skills, oral questioning, written questions, case studies, assignments, projects and RPL.

To be able to assess both knowledge and competence-based qualifications, new assessors should be working towards the **Level 3 Certificate in Assessing Vocational Achievement.**

Centres must have in place a procedure to ensure that their trainee assessors have a representative sample of their assessment decisions counter signed by a qualified and competent assessor. SFJ Awards will provide centres with guidance on the ratio of qualified/trainee assessors.

Trainee assessors working towards a qualification must be registered for the qualification with a regulated AO and achieve it within 18 months. Assessor competence will be checked through annual External Quality Assurance checks.

Centres must check the qualification handbook for assessor requirements for the qualification(s) they are approved to deliver as some sectors have different requirements e.g. security, education and training, assessor and quality assurance, and learning and development.

Centres applying for approval with SFJ Awards will be required to provide SFJ Awards with current evidence of how each assessor meets these requirements, for example certificates of achievement. Centres who apply for approval to offer additional qualifications will be required to provide evidence of assessor competence for the qualifications they wish to offer.

6.4. Continuing Professional Development

Assessors must actively engage in continuous professional development activities to maintain:

- occupational competence and knowledge by keeping up-to-date with the changes taking place in the sector(s) for which they carry out assessments
- professional competence and knowledge as an assessor.

It is the centre's responsibility to retain the CPD information of assessors. Assessor competence and CPD will be checked by External Quality Assurers at the centre's annual compliance visit.

7. Internal Quality Assurer Requirements

7.1. Occupational Knowledge

Internal quality assurers (IQAs) must be occupationally knowledgeable across the range of units for which they are responsible prior to commencing the role. Due to the risk-critical nature of the work, particularly in the justice, community safety and security sectors, and the legal implications of the assessment process, they must understand the nature and context of the assessors' work and that of their learners. This means that they must have worked closely with staff who carry out the functions covered by the qualifications, possibly by training or supervising them, and have sufficient knowledge of these functions to be able to offer credible advice on the interpretation of the units.

7.2. Qualification Knowledge

IQAs must understand the content, structure and assessment requirements for the qualification(s) they are internal quality assuring.

Centres should provide IQAs with an induction to the qualifications that they are responsible for quality assuring. IQAs should also have access to ongoing training and updates on current issues relevant to these qualifications.

7.3. Internal Quality Assurer Competence

IQAs must occupy a position in the organisation that gives them the authority and resources to:

- coordinate the work of assessors
- provide authoritative advice
- call meetings as appropriate
- conduct pre-delivery internal quality assurance on centre assessment plans, for example, to ensure that any proposed simulations are fit for purpose
- visit and observe assessment practice
- review the assessment process by sampling assessment decisions
- ensure that assessment has been carried out by assessors who are occupationally competent, or for knowledge-based qualifications occupationally knowledgeable, in the area they are assessing
- lead internal standardisation activity
- resolve differences and conflicts on assessment decisions

To demonstrate their competence, IQAs must be:

- qualified with a recognised internal quality assurance qualification, or
- working towards a recognised internal quality assurance qualification.

However, there may be circumstances when IQAs have the equivalent competence through training to appropriate national standards, and SFJ Awards will agree this on a case-by-case basis. Recognised IQA qualifications include, but are not limited to:

- RQF/QCF Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice
- RQF/QCF Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practice
- An appropriate IQA qualification in the SCQF as identified by SQA Accreditation
- V1 Conduct internal quality assurance of the assessment process
- D34 Internally verify the assessment process.

Where IQAs hold an older qualification e.g. D34 or V1, they must provide evidence of Continuing Professional Development (CPD) to demonstrate current competence. Approved centres will be required to provide SFJ Awards with current evidence of how each IQA meets these requirements, for example certificates of achievement.

Centres must have in place a procedure to ensure that their trainee IQAs have a representative sample of their IQA decisions counter signed by a qualified IQA who holds a minimum of the **Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice**. SFJ Awards will provide centres with guidance on the ratio of qualified/trainee assessors.

Trainee IQAs working towards one of the above qualifications must be registered for the qualification with a regulated AO and achieve it within 18 months. IQA competence will be checked through annual External Quality Assurance checks.

7.4. Continuing Professional Development

IQAs must actively engage in continuous professional development activities to maintain:

- occupational knowledge by keeping up-to-date with the changes taking place in the sector(s) for which they carry out assessments
- professional competence and knowledge as an IQA.

Centres must check the qualification handbook for IQA requirements for the qualification(s) they are approved to deliver as some sectors have different requirements e.g. security, education and training, assessor and quality assurance, and learning and development.

8. Expert Witnesses

Expert witnesses, for example line managers and supervisors, can provide evidence that a learner has demonstrated competence in an activity. Their evidence contributes to performance evidence and has parity with assessor observation. Expert witnesses do not however perform the role of assessor.

8.1. Occupational Competence

Expert witnesses must, according to current sector practice, be competent in the functions covered by the unit(s) for which they are providing evidence.

They must be able to demonstrate consistent application of the skills and the current supporting knowledge and understanding in the context of a recent role directly related to the qualification unit that they are witnessing as a practitioner, trainer or manager.

8.2. Qualification Knowledge

Expert witnesses must be familiar with the qualification unit(s) and must be able to interpret current working practices and technologies within the area of work.

9. External Quality Assurers

External quality assurance is carried out by SFJ Awards to ensure that there is compliance, validity, reliability and good practice in centres. External quality assurers (EQAs) are appointed by SFJ Awards to approve centres and to monitor the assessment and internal quality assurance carried out by centres.

SFJ Awards are responsible for ensuring that their external quality assurance team have:

- sufficient and appropriate occupational knowledge
- current experience of external quality assurance
- access to appropriate training and support.

9.1. External Quality Assurer Competence

To demonstrate their competence, EQAs must be:

- qualified with a recognised external quality assurance qualification, or
- working towards a recognised external quality assurance qualification

Relevant qualifications include:

- Level 4 Award in the External Quality Assurance of Assessment Processes and Practice
- Level 4 Certificate in Leading the External Quality Assurance of Assessment Processes and Practice

Trainee EQAs working towards one of the above qualifications must be registered for the qualification with a regulated AO and aim to achieve it within 18 months. Whilst working towards a qualification, trainee EQAs will be supported by qualified EQA and receive training, for example by shadowing the EQA on compliance visits. EQA competence will be checked and monitored by SFJ Awards.

9.2. Continuing Professional Development

EQAs must maintain their occupational and external quality assurance knowledge. They will attend training and development designed to keep them up-to-date, facilitate standardisation between staff and share good practice.

10. Standardisation

Internal and external standardisation is required to ensure the consistency of evidence, assessment decisions and qualifications awarded over time.

10.1. Internal Standardisation

IQAs should facilitate internal standardisation events for assessors to attend and participate, in order to review evidence used, make judgments, compare quality and come to a common understanding of what is sufficient.

10.2. External Standardisation

SFJ Awards will enable access to external standardisation opportunities for centres and EQAs over time.

Further information on standardisation is available in the SFJ Awards Quality Assurance (Internal and External) Guidance and the SFJ Awards Standardisation Policy.

11. Recognition of Prior Learning (RPL)

Recognition of prior learning (RPL) is the process of recognising previous formal, informal or experiential learning so that the learner avoids having to repeat learning/assessment within a new qualification. RPL is a broad concept and covers a range of possible approaches and outcomes to the recognition of prior learning (including credit transfer where an Awarding Organisation has decided to attribute credit to a qualification).

The use of RPL encourages transferability of qualifications and/or units, which benefits both learners and employers. SFJ Awards support the use of RPL and centres must work to the principles included in Section 6 Assessment and Quality Assurance of the SFJ Awards Centre Handbook and outlined in SFJ Awards Recognition of Prior Learning Policy.

12. Equality and Diversity

Centres must comply with legislation and the requirements of the RQF relating to equality and diversity. There should be no barriers to achieving a qualification based on:

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

Reasonable adjustments are made to ensure that learners who are disabled or who have additional learning needs are not disadvantaged in any way. Learners must declare their needs prior to the assessment and all necessary reasonable adjustment arrangements must have been approved by SFJ Awards and implemented before the time of their assessment.

All cases where reasonable adjustment has been used must be fully documented, made available for external quality assurance and retained for a minimum of 3 years.

Further information is available in the SFJ Awards Reasonable Adjustments and Special Considerations Policy and the SFJ Awards Equality of Opportunity Policy.

SFJ Awards will conduct Equality Impact Assessments in the design and development of qualifications to minimise as far as possible any impact on learners with a protected characteristic, disability or additional learning needs.

13. Health and Safety

SFJ Awards are committed to safeguarding and promoting the welfare of learners, employees and volunteers and expect everyone to share this commitment.

SFJ Awards foster an open and supportive culture to encourage the safety and well-being of employees, learners and partner organisations to enable:

- learners to thrive and achieve
- employees, volunteers and visitors to feel secure
- everyone to feel assured that their welfare is a high priority.

Assessment of competence-based qualifications in some sectors can carry a high risk level due to the nature of some roles. Centres must therefore ensure that due regard is taken to assess and manage risk and have procedures in place to ensure that:

- qualifications can be delivered safely with risks to learners and those involved in the assessment process minimised as far as possible
- working environments meet relevant health and safety requirements.

Copyright

SFJ Awards
Consult House
4 Hayland Street
Sheffield S9 1BY
Tel: 0114 284 1970
sfjawards.com