



Diploma in Cyber Security (SCQF Level 8)

QUALIFICATION SUMMARY

FROM SEPTEMBER 2026
ISSUE 1.0

Contents

1	Introduction and Summary.....	1
2	Aims	1
3	Teaching, Learning and Assessment.....	1
4	Entry Requirements	2
5	Recognition of Prior Learning (RPL).....	2
6	Progression.....	2
7	Curriculum	3
8	National Occupational Standards (NOS)	4
9	Learning / teaching methods and strategies	4
10	Assessment Methods and Strategies	5

1 Introduction and Summary

The EduQual Diploma in Cyber Security (SCQF Level 8) is a Qualification equivalent to a Regulated Qualifications Framework (RQF) Qualification at Level 5. It offers Learners the knowledge and skills needed to develop an understanding of the models, tools and techniques used in the field of cyber security. The Qualification has been mapped to the National Occupational Standards in cyber security, and Learners will be able to develop the competencies they need to enter work in this discipline.

Holders of the EduQual Diploma in Cyber Security (SCQF Level 8) may be considered (by UK Higher Education Institutions e.g. universities) for progression, with advanced standing (academic credit), onto degree programmes.

The Qualification has been produced to conform to the requirements of the RQF.

2 Aims

The aims of this Qualification will enable Learners to:

- Build a coherent and sound foundation in cyber security, at a level equivalent to a Higher National Diploma, enabling graduates to choose from a wide range of career options internationally within the cyber security discipline¹
- Pursue a specialist interest in cyber security and relate this expertise to professional requirements and codes of conduct in line with the National Occupational Standards (NOS)
- Develop a wide range of intellectual and analytical abilities relevant to cyber security, including those of critical thinking and analytical decision making
- Develop and practice the transferable skills necessary for continual personal development and to respond positively to change during careers in cyber security
- Discuss terminology, concepts, principles and techniques as utilised in cyber security
- Explain the importance of the social, political, ethical, technological, environmental and global contexts in which cyber security organisations operate and to support small- and medium-sized business enterprise (SME) decision making
- Develop the attitudes, skills and abilities necessary to work in an international cyber security context and an awareness and appreciation of different cultural values
- Prepare for further studies at degree level

3 Teaching, Learning and Assessment

Teaching and learning will be undertaken using a range of face-to-face learning, whether online or through tutor directed study, lectures, seminars and tutorials. Learners will be encouraged to develop their skills in self-directed learning, which will take place outside the formal classroom environment.

¹ For example: SOC Analyst, Information Security Analyst, IT Support Specialist, Penetration Testing Specialist, and System Administrator

Formative assessments will arise through projects, case studies, research and testing wherever appropriate.

Summative assessment will be through responses to assignments enabling Learners to demonstrate their understanding of the subjects they have studied.

4 Entry Requirements

Prospective Learners for this Qualification are expected to have:

- GCSE in English and Mathematics (Grade C or above) or equivalent
- 200 points from two subjects at GCE A-Level or equivalent

Equivalent Qualification(s) will be considered

Applications from mature Learners and those offering Qualifications other than GCE A-Levels are welcomed and will be considered on an individual basis.

Applicants for whom English is not a first language will be expected to demonstrate a certified level of proficiency of at least IELTS (International English Language Testing System) 6 or above.

In exceptional circumstances and at the discretion of the Centre, Learners who do not have any of the prescribed entry requirements may still be permitted to study for the Qualification, provided that in the Centre's judgement, the Learner has the potential to complete the Qualification successfully. Centres should consult the Access and Recruitment Section of the Qualification Specification document.

5 Recognition of Prior Learning (RPL)

RPL (sometimes referred to as APL) may be claimed by a Learner in situations where:

- The Learner has already studied SCQF-equivalent Level 7 or 8 Units that are also equivalent to the Learning Outcomes of the Units of this Qualification.
- The Learner can also produce evidence to demonstrate how each of the assessment criteria have already been met.

In such a case, those matching Units can be exempted from study, credits can be claimed, and the evidence supporting the RPL claim can be included in the Learner's portfolio of evidence when claiming the Award.

6 Progression

Holders of the EduQual Diploma in Cyber Security (SCQF Level 8) may be considered (by UK Higher Education Institutions e.g. universities) for progression, with advanced standing (academic credit), onto degree programmes.

7 Curriculum

The EduQual Diploma in Cyber Security is an SCQF Level 8 (RQF equivalent Level 4) Qualification consisting of **TWELVE** Units, all of which are compulsory, as shown:

Diploma in Cyber Security (SCQF Level 8) Compulsory Units		
Unit Title	SCQF Level	Credits
Unit 1: Cyber Security Fundamentals	7	20
Unit 2: Introduction to Computing	6	20
Unit 3: Introduction to Programming	7	20
Unit 4: Database Management	7	20
Unit 5: Digital Forensics	8	20
Unit 6: Web Programming	8	20
Unit 7: Networking Administration	8	20
Unit 8: AI in Cyber Security	8	20
Unit 9: Intrusion Analysis	7	20
Unit 10: Cyber Resilience	8	20
Unit 11: Computer Software Engineering	8	20
Unit 12: Advanced Programming	8	20
Total Credits		240

8 National Occupational Standards (NOS)

Some Units in the EduQual Diploma in Cyber Security relate to the National Occupational Standards for cyber security. For more information on how these Units relate to NOS Units in cyber security, please contact us at info@eduqual.org.uk.

9 Learning / teaching methods and strategies

The Learning Outcomes will be achieved by the use of the following learning and teaching methods and strategies:

- A variety of teaching and learning strategies, including lecture, seminar, case study and video.
- Team teaching on specific modules to foster integration between various aspects of cyber security.
- Independent and group activities (class and non-class based) through which good practice can be shared and exchanged.
- Live and simulated case studies.
- Speakers and subject specialists.
- Personal and professional self-reflection, including feedback from colleagues and superiors.
- The creation of a learning environment that fosters debate and constructive argument.
- Units which encourage Learners to assess theory and leading-edge practice, with a view to creating new concepts and practices for the future.
- Practical projects which foster originality of thought and enterprise.
- Learner Management Systems (online platforms for delivering, tracking, and managing educational courses or training programmes)

10 Assessment Methods and Strategies

The following assessment strategies will be adopted to achieve the Learning Outcomes:
Assessments in the form of management reports with a strong practical and professional orientation to the workplace may include:
• Case studies which examine key issues within cyber security • Group presentations which present arguments in a coherent and insightful manner • Project work carried out and reported upon based on work experience
Formative assessment may include:
• Peer review of work between individuals and groups • Material presented in class – either individually or as a group – where clarity of argument and evidence is supported with appropriate references • Feedback in class situations on topics of current interest • Evidence of breadth of research, including internet sources, where appropriate to the curriculum topics covered
Summative assessment may be by assignment which may include work such as:
• Observation of performance in the work environment • Examining products of work, such as: ○ Individual or group presentations which coherently and concisely present analysis of cyber security issues ○ Examination (seen or unseen) ○ Coursework assignments (including problem solving activities, simulations, consultancy projects, individual and group reports, as well as more conventional written forms such as essays and other discursive assignments) • Questioning the Learner • Reflective forms of assessment (e.g. portfolios, Learner logs, and peer engagement).