Skills & Education Group Awards

In association with UK AWARDS Education Excellence

Qualification Guidance

SEG Awards Level 5 Diploma in Software Engineering with Cyber Security

England – 610/4137/3

Qualification Guidance

About Us

At Skills and Education Group Awards we continually invest in high quality qualifications, assessments and services for our chosen sectors. As a UK leading sector specialist, we continue to support employers and skills providers to enable individuals to achieve the skills and knowledge needed to raise professional standards across our sectors.

Skills and Education Group Awards has an on-line registration system to help customers register learners on its qualifications, units and exams. In addition, it provides features to view exam results, invoices, mark sheets and other information about learners already registered.

The system is accessed via a web browser by connecting to our secure website using a username and password:

Skills and Education Group Awards Secure Login

Sources of Additional Information

Skills and Education Group Awards website www.skillsandeducationgroupawards.co.uk provides access to a wide variety of information.

Copyright

Specification Code

The specification code is D5061-05.

Issue	Date	Details of change
1.0	May 2024	New qualification guide

This guide should be read in conjunction with the Indicative Content document which is available on our secure website using the link above.

Skills & Education Group Awards

Qualification Guidance

Contents

This is a live document and as such will be updated when required. It is the responsibility of the approved centre to ensure the most up-to-date version of the Qualification Guide is in use. Any amendments will be published on our website and centres are encouraged to check this site regularly.

Skills & Education Group Awards

Qualification Guidance

Introduction

The SEG Level 5 Diploma in Software Engineering with Cyber Security aims to develop competence as a software developer. It is designed to provide an education that will develop knowledge and understanding of relevant theories and principles together with technical skills and capabilities associated with the practice of the discipline.

Learners will learn to plan, design, program, manage and test software applications and develop an understanding of the software design process. This will support development throughout a learners career. The aim of any programme of study in software engineering should be to develop expertise in software development.

The key areas covered include:

- Incident Response and Intrusion Detection
- Web Application Development
- Software Project Management
- Object-Oriented Design and Development
- Ethical Hacking
- Software Project

The knowledge and skills gained will prepare learners to progress onto higher programmes of study, and related qualifications, in Computing and Information Technology.

Pre-requisites

There are no entry requirements for this qualification. However, learners should be working to at **least** Level 3.

Skills and Education Group Awards expects approved centres to recruit with integrity on the basis of a trainee's ability to contribute to and successfully complete all the requirements of a unit(s) or the full qualification.

Skills & Education Group Awards

Qualification Guidance

Qualification Structure and Rules of Combination

Rules of Combination: Level 5 Diploma in Software Engineering with Cyber Security

Learners must achieve **all** 120 credits from **all** the 6 mandatory units.

Unit	Unit Number	Level	Credit Value	GL
Mandatory Group Min Credit Target - 120				
Incident Response and Intrusion Detection	D/651/1384	5	20	80
Web Application Development	A/651/1077	5	20	80
Software Project Management	D/651/1078	5	20	80
Object-Oriented Design and Development	F/651/1079	5	20	80
Ethical Hacking	F/651/1385	5	20	80
Software Project	L/651/1081	5	20	80

Aims

Upon successful completion of the SEG Awards Level 5 Diploma in Software Engineering with Cyber Security, learners will be able to:

- Develop knowledge of some of the technologies and processes used in the modern software development
- Demonstrate an awareness of modern software development methodologies and their role in software development
- Analyse client requirements to develop and test software solutions based on client requirements
- Program object-oriented applications for a web-based system which uses a database system
- Work effectively in a team environment
- Communicate effectively in written and oral form

Skills & Education Group Awards

Qualification Guidance

Target Group

The SEG Awards Level 5 Diploma in Software Engineering with Cyber Security is designed for learners, **16 years of age and over**, who are looking to develop competence as a software developer. It is designed to provide an education that will develop knowledge and understanding of relevant theories and principles together with technical skills and capabilities associated with the practice of the discipline.

Assessment

The curriculum is set up to support a portfolio approach to continuous assessment. Learners will study modules and develop a portfolio of evidence. Each module will have milestones where formative assessment is provided, and learners can then continue to work on their portfolios before a final submission at the end of the module.

For each module, an assessment grid is provided indicating the learning outcomes to be achieved and the evidence required to support their attainment. This grid contains evidence requirements for grading at pass, merit, and distinction. The criteria are cumulative, so to achieve a merit grade a learner must satisfy the criteria for both a pass and for a merit. Similarly, to achieve a distinction grade a learner must satisfy, pass, merit, and distinction criteria.

To achieve a pass in a module, a pass grade must be attained for all learning outcomes. The overall grade for each module will be determined by the predominant attainment in each of the learning outcomes. For example, most modules have four learning outcomes so if three are attained at merit, then a merit grade is the outcome. If the outcome is that two learning outcomes are graded pass and two at merit, then a merit for the module would be awarded. For a distinction grade, the predominant attainment in each of the learning outcomes must be at distinction grade with all learning outcomes achieving at least a merit grade.

For the diploma to be awarded, a pass grade must be achieved in all modules. The overall grade for the diploma will be determined based on the predominant outcome for each of the modules. There are six modules, so to achieve an overall grade of merit at least three modules must be graded at merit. To achieve a distinction, all modules must be graded at minimum of merit and at least three at distinction.

Practice Assessment Material

Skills and Education Group Awards confirm that there is no practice material available for the SEG Awards Level 5 Diploma in Software Engineering with Cyber Security.

Teaching Strategies and Learning Activities

The fundamental philosophy that guides this curriculum is project based learning with a balance between the following elements.

- Lectures and lessons – where knowledge is acquired
- Seminars and tutorials – where knowledge is consolidated and know-how developed
- Laboratories – where practical skills are demonstrated and developed
- Projects – where learners can develop their skills of synthesis

Centres should adopt a delivery approach which supports the development of all individuals. The aims and aspirations of all the learners, including those with identified special needs or learning difficulties/disabilities, should be considered and appropriate support mechanisms put in place.

Progression Opportunities

Learners who achieve this qualification could progress onto further Level 5 and Level 6 qualifications in IT, Computing and Software. Learners could also progress into employment.

Centres should be aware that Reasonable Adjustments which may be permitted for assessment may in some instances limit a learner's progression into the sector. Centres **must**, therefore, inform learners of any limits their learning / physical difficulty may impose on future progression.

Tutor / Assessor Requirements

Skills and Education Group Awards require those involved in the teaching and assessment process to be suitably qualified. Assessors should also be trained and qualified to assess or be working towards appropriate teaching qualifications.

Qualification Guidance

Minimum requirements when delivering this qualification: Skills and Education Group Awards expects that staff will be appropriately qualified to assess learners against the outcomes and criteria within the units. Teaching staff **must** be qualified at least a level above in a relevant subject to which they are teaching.

Those responsible for Internal Quality Assurance (IQA) **must** be knowledgeable and or qualified of the subject/occupational area to a suitable level to carry out accurate quality assurance practices and processes.

Language

This specification and associated assessment materials are in English only.

Qualification Guidance

Qualification Summary

Qualification									
SEG Awards Level 5 Diploma in Software Engineering with Cyber Security									
Qualification Purpose	Prepare for further learning or training and/or develop knowledge and/or skills in a subject area								
Age Range	**Pre 16**		**16-18**	✓	**18+**	✓	**19+**	✓	
Regulation	The above qualification is regulated by: • Ofqual								
Assessment	• Portfolio of Evidence								
Type of Funding Available	See FaLA (Find a Learning Aim)								
Grading	Pass/Merit/Distinction/Fail								
Operational Start Date	01/05/2024								
Review Date	01/05/2027								
Operational End Date	-								
Certification End Date	-								
Guided Learning (GL)	480 hours								
Total Qualification Time (TQT)	1200 Hours								
Credit Value	120								
Skills and Education Group Awards Sector	Computing and Software								
Regulator Sector	6.1 ICT Practitioners								
Support from Trade Associations	-								

Skills & Education Group Awards

Qualification Guidance

Unit Details

Incident Response and Intrusion Detection

Unit Reference	**D/651/1384**	
Level	**5**	
Credit Value	**20**	
Guided Learning (GL)	**80 hours**	
Unit Summary	In this unit learners will be introduced to the practical tools required to respond to a cyber security incident. Learners will also apply appropriate intrusion detection and incident response approaches to mitigate cyber-attacks against the organisation.	
Unit Aim	The learner should develop a portfolio based on a company or organisation in their country or a case study identified by their tutors.	
Learning Outcomes (1 to 4)	**Assessment Criteria (1.1 to 4.4)**	
The learner will	***The learner can***	
1. Understand the concepts and features of intrusion detection, prevention and response	1.1	Define the following: a) intrusion detection b) prevention c) response
	1.2	Analyse the key features of the systems defined in 1.1
	1.3	Compare and contrast techniques used in: a) intrusion detection b) prevention c) response techniques
2. Understand what constitutes evidence of malicious behaviour when examining network traffic, both in real-time or captured format	2.1	Explain patterns indicative of malicious behaviour in network traffic
	2.2	Evaluate methods for detecting and interpreting anomalies in network traffic

Qualification Guidance

	2.3	Explain how to identify and document evidence of malicious activity in both real-time and captured network traffic
3. Be able to collect, analyse (including through the use of appropriate mathematical and statistical concepts) and evaluate digital evidence	3.1 3.2 3.3	Collect digital evidence from various sources Apply mathematical and statistical concepts to analyse digital evidence effectively Evaluate the reliability and relevance of digital evidence in a given context
4. Be able to apply the concepts and features of intrusion detection, prevention and incident response	4.1 4.2 4.3 4.4	Implement intrusion detection, prevention, and incident response strategies in a simulated scenario Analyse real-world incidents applying appropriate intrusion detection, prevention, and response techniques Develop incident response plans based on identified threats and vulnerabilities Using a given scenario carry out the plans developed in 4.3

Skills & Education Group Awards

Qualification Guidance

Web Application Development

Unit Reference	**A/651/1077**	
Level	**5**	
Credit Value	**20**	
Guided Learning (GL)	**80 hours**	
Unit Summary	This unit develop a learners understanding of tools, technologies and techniques which enable web browsers to host interactive applications and manage data in those applications.	
Unit Aim	The learner should develop a portfolio based on their learning.	
Learning Outcomes (1 to 4)	**Assessment Criteria (1.1 to 4.4)**	
The learner will	***The learner can***	
1. Understand the components, processes and technologies behind an interactive web application	1.1	Identify key components necessary for interactive web applications including: a) client-side scripts b) server-side technologies
	1.2	Describe the processes involved in developing and maintaining interactive web applications, including data handling and security measures
	1.3	Explain the technologies commonly used in interactive web application development, including: a) HTML b) CSS c) JavaScript d) backend frameworks
2. Develop an interactive web application using modern tools and techniques	2.1	Design a user-friendly interface that incorporates responsive design principles
	2.2	Use front-end functionalities using HTML, CSS, and JavaScript

Qualification Guidance

	2.3	Utilise appropriate frameworks to improve interactivity
	2.4	Demonstrate that the web application is cross-browser compatible for a seamless user experience
3. Understand what responsive applications are and assess the quality of the interface of a web based interactive application	3.1	Explain the concept of responsive design and its importance in creating adaptable interfaces
	3.2	Evaluate the responsiveness of a web application across different devices and screen sizes
	3.3	Analyse the accessibility features implemented in the interface for a diverse user base
	3.4	Critically assess the user experience design elements for intuitive navigation and interaction
4. Understand the importance of security and demonstrate how security techniques can be applied to an interactive web-based application	4.1	Identify potential security threats and vulnerabilities in web applications
	4.2	Explain how secure communication protocols such as HTTPS protects data in transit
	4.3	Integrate authentication mechanisms like OAuth or JWT for user verification
	4.4	Discuss the importance of conducting regular security audits and testing to ensure the application is resilient to attacks

Skills & Education Group Awards

Qualification Guidance

Software Project Management

Unit Reference	**D/651/1078**	
Level	**5**	
Credit Value	**20**	
Guided Learning (GL)	**80 hours**	
Unit Summary	In this unit learners will develop their understanding of Project Management approaches and procedures that can be applied to a range of organisational situations. Project management helps with effective planning and control of projects by using appropriate Project Management software.	
Unit Aim	The learner should develop a portfolio based on their learning.	
Learning Outcomes (1 to 3)	**Assessment Criteria (1.1 to 3.4)**	
The learner will	***The learner can***	
1. Understand the factors contributing to the success (or failure) of IT ventures at both the project and organisational level	1.1	Analyse key success factors in IT ventures, distinguishing between project and organisational levels
	1.2	Evaluate the impact of identified success factors on the outcomes of IT projects
	1.3	Analyse factors that can lead to the failure of IT ventures
	1.4	Critically evaluate the relationship between project success and organisational success in IT ventures

Qualification Guidance

2. Be able to identify and reflect on the actions or measures that may be taken to minimise the failure of a computing project	2.1	Identify proactive measures to prevent project failure in computing projects
	2.2	Reflect on potential risk mitigation strategies to minimise project failure in a computing environment
	2.3	Propose actionable steps to address and mitigate project failure risks in computing projects
	2.4	Evaluate the effectiveness of proposed measures in minimising project failure within computing projects
3. Understand the software life cycle, its processes, and application	3.1	Describe the stages of the software life cycle and their sequential order
	3.2	Explain the key processes involved in each phase of the software life cycle
	3.3	Apply the concepts of the software life cycle to a practical project scenario
	3.4	Analyse the impact of effectively implementing the software life cycle on project outcomes

Skills & Education Group Awards

Qualification Guidance

Object-Oriented Design and Development

Unit Reference	**F/651/1079**
Level	**5**
Credit Value	**20**
Guided Learning (GL)	**80 hours**
Unit Summary	In this unit learners will develop their programming skills by utilising object-oriented design and development approaches. Learners will apply agile development approaches to application development. Learners will learn a topical object-oriented programming language during the module, which they can use to develop a software application.
Unit Aim	The learner should develop their websites based on an industry case study identified by their tutors.

Learning Outcomes (1 to 4)	**Assessment Criteria (1.1 to 4.4)**	
The learner will	***The learner can***	
1. Understand the fundamental Object-Orientated (OO) principles (such as encapsulation, inheritance and polymorphism) and concepts (such as classes, objects and message passing) and describe their importance in software reuse, and maintenance	1.1	Explain the following conception Object-Oriented programming: a) encapsulation b) inheritance c) polymorphism
	1.2	Identify the significance of the following in software design: a) classes b) objects c) message passing
	1.3	Discuss how fundamental OO principles contribute to software reuse and maintenance
	1.4	Analyse the impact of using OO concepts on enhancing software scalability and maintainability

Qualification Guidance

2. Be able to use a suitable programming language to develop an efficient and reusable OO software application	2.1	Develop an OO software application using a chosen programming language
	2.2	Use efficient coding practices to optimise the performance of the software application
	2.3	Demonstrate the reusability of code components within the OO software application
	2.4	Evaluate the effectiveness of the chosen programming language in facilitating OO design principles for the software application
3. Be able to identify, implement and use appropriate underlying data structures to store and manipulate data in an OO program	3.1	Identify suitable data structures for storing and manipulating data in an OO program
	3.2	Implement the identified data structures effectively within the OO program
	3.3	Demonstrate the use of the chosen data structures to manipulate data accurately
	3.4	Evaluate the efficiency of the selected data structures in terms of performance and scalability within the OO program
4. Understand the benefits of software reuse and the limitations of using objects software applications	4.1	Explain the advantages of software reuse in developing object-oriented software applications
	4.2	Discuss the limitations associated with utilising objects in software development
	4.3	Analyse how software reuse can enhance productivity and efficiency in software development
	4.4	Evaluate the potential challenges and drawbacks of relying on object-oriented design in software applications

Ethical Hacking

Unit Reference	**F/651/1385**	
Level	**5**	
Credit Value	**20**	
Guided Learning (GL)	**80 hours**	
Unit Summary	In this learners will be introduced to key concepts in ethical hacking such as blue team, red team and purple team hacking. Learners will identify, exploit and mitigate security vulnerabilities and understand the legal, social, ethical and professional issues surrounding ethical hacking.	
Unit Aim	The learner should develop their programs based on a case study identified by their tutors.	
Learning Outcomes (1 to 4)	**Assessment Criteria (1.1 to 4.4)**	
The learner will	***The learner can***	
1. Understand the phases in ethical hacking and the approaches available to a cyber security professional	1.1	Explain the phases involved in ethical hacking
	1.2	Describe different approaches used by cyber security professionals in ethical hacking
	1.3	Compare and contrast various ethical hacking methodologies and their applications

Qualification Guidance

2. Know how to identify and evaluate vulnerabilities in computer systems, networks and web applications	2.1	Identify vulnerabilities in computer systems, networks, and web applications
	2.2	Evaluate the severity and potential impact of identified vulnerabilities
	2.3	Use appropriate tools and techniques to assess the security posture of the following: a) computer systems b) networks c) web applications
3. Be able to test and find solutions to vulnerabilities in computing systems, networks and web applications	3.1	Conduct comprehensive vulnerability assessments using industry-standard tools, on the following: a) computing systems b) networks c) web applications
	3.2	Develop detailed reports outlining identified vulnerabilities, their potential impact, and recommended solutions
	3.3	Implement effective remediation strategies to address vulnerabilities, ensuring the security and integrity of computing systems, networks, and web applications
	3.4	Evaluate the effectiveness of implemented solutions through rigorous testing and validation procedures
4. Be able to analyse legal, social, ethical and professional issues in ethical hacking	4.1	Examine the legal frameworks governing ethical hacking practices, identifying relevant regulations and compliance requirements
	4.2	Critically evaluate the social and ethical implications of ethical hacking activities on individuals, organisations, and society as a whole

	4.3	Assess the professional responsibilities and ethical considerations associated with ethical hacking activities, including confidentiality, integrity, and professionalism
	4.4	Analyse the ethical dilemmas and moral complexities inherent in ethical hacking, demonstrating an understanding of ethical decision-making frameworks

Skills & Education Group Awards

Qualification Guidance

Software Project

Unit Reference	**L/651/1081**
Level	**5**
Credit Value	**20**
Guided Learning (GL)	**80 hours**
Unit Summary	This unit provides learners an opportunity to develop and evidence their ability to work as a member of a team in the planning, management, development, testing and delivery. The unit also covers key social, legal, ethical and professional concepts while implementing a software project. Learners will build on their knowledge from the first-year software project module and other technical units studied in the second year of study to bring together knowledge of web development, software engineering, mobile application development and databases to produce a software system.
Unit Aim	The learner should develop a portfolio based on a company or organisation in their country or a case study identified by their tutors.
Learning Outcomes (1 to 4)	**Assessment Criteria (1.1 to 4.5)**
The learner will	***The learner can***
1. Be able to analyse an outline of a problem brief and determine a specification, plan, processes, resources and tools to undertake a programme of work for the project	1.1 Develop a detailed project specification aligning with the outlined problem brief 1.2 Create a comprehensive project plan outlining key milestones and deliverables 1.3 Identify suitable processes to be implemented throughout the project lifecycle

	1.4	Select appropriate resources and tools necessary to carry out the programme of work effectively
2. Be able to apply professional, social, legal, and ethical codes of conduct, practices and responsibilities and safety/security related issues related to your project work	2.1	Explain the importance of adhering to professional codes of conduct throughout project activities
	2.2	Apply legal and ethical principles to decision-making processes within the project
	2.3	Use safety and security measures in all project-related tasks
	2.4	Discuss social responsibilities associated with the project work
3. Understand the key concepts of data confidentiality, integrity and availability	3.1	Examine the importance of data confidentiality in project environments
	3.2	Analyse the significance of maintaining data integrity in software projects
	3.3	Identify strategies to ensure data availability throughout project execution
	3.4	Explain the interplay between data confidentiality, integrity, and availability in project contexts
4. Be able to deploy appropriate theory, practices, and tools to analyse, specify, test, implement and evaluate systems, using appropriate development approaches to scope, time-manage and organise a project	4.1	Explain the importance of using appropriate development approaches to scope, time-manage and organise a project
	4.2	Apply relevant theoretical frameworks to analyse system requirements effectively
	4.3	Specify clear and achievable objectives for system testing procedures
	4.4	Implement system components in accordance with specified requirements

	4.5	Evaluate system performance against predefined criteria recommending improvements where necessary

Recognition of Prior Learning (RPL), Exemptions, Credit Transfers and Equivalencies

Skills and Education Group Awards policy enables learners to avoid duplication of learning and assessment in a number of ways:

- Recognition of Prior Learning (RPL) – a method of assessment that considers whether a learner can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and do not need to develop through a course of learning.
- Exemption - Exemption applies to any certificated achievement which is deemed to be of equivalent value to a unit within Skills and Education Group Awards qualification but which does not necessarily share the exact learning outcomes and assessment criteria. It is the assessor's responsibility, in conjunction with the Internal Moderator, to map this previous achievement against the assessment requirements of the Skills and Education Group Awards qualification to be achieved in order to determine its equivalence. Any queries about the relevance of any certificated evidence, should be referred in the first instance to your centre's internal moderator and then to Skills and Education Group Awards.
  It is important to note that there may be restrictions upon a learner's ability to claim exemption or credit transfer which will be dependent upon the currency of the unit/qualification and a learner's existing levels of skill or knowledge.
  Where past certification only provides evidence that could be considered for exemption of part of a unit, learners must be able to offer additional evidence of previous or recent learning to supplement their evidence of achievement.
- Credit Transfer – Skills and Education Group Awards may attach credit to a qualification, a unit or a component. Credit transfer is the process of using certificated credits achieved in one qualification and transferring that achievement as a valid contribution to the award of another qualification. Units/Components transferred must share the same learning outcomes and assessment criteria along with the same unit number. Assessors must ensure that they review and verify the evidence through sight of:
  - Original certificates OR
  - Copies of certificates that have been signed and dated by the internal moderator confirming the photocopy is a real copy and make these available for scrutiny by the External Moderator.
- Equivalencies – opportunities to count credits from the unit(s) from other qualifications or from unit(s) submitted by other recognised organisations towards the place of mandatory or optional unit(s) specified in the rule of combination. The unit must have the same credit value or greater than the unit(s) in question and be at the same level or higher.

Skills and Education Group Awards encourages its centres to recognise the previous achievements of learners through Recognition of Prior Learning (RPL),

Exemption, Credit Transfer and Equivalencies. Prior achievements may have resulted from past or present employment, previous study or voluntary activities. Centres should provide advice and guidance to the learner on what is appropriate evidence and present that evidence to the external moderator in the usual way.

Further guidance can be found in 'Delivering and Assessing Skills and Education Group Awards Qualifications' which can be downloaded from https://skillsandeducationgroupawards.co.uk/for-centres/

Certification

Learners will be certificated for all units and qualifications that are achieved and claimed.

Skills and Education Group Awards' policies and procedures are available on the website.

Exemptions

This qualification contains no exemptions. For further details see Recognition of Prior Learning (RPL), Exemptions, Credit Transfers and Equivalencies.

Glossary of Terms

GL (Guided Learning)
GL is where the learner participates in education or training under the immediate guidance or supervision of a tutor (or other appropriate provider of education or training). It may be helpful to think – 'Would I need to plan for a member of staff to be present to give guidance or supervision?'

GL is calculated at qualification level and not unit/component level.

Examples of Guided Learning include:

- Face-to-face meeting with a tutor
- Telephone conversation with a tutor
- Instant messaging with a tutor
- Taking part in a live webinar
- Classroom-based instruction
- Supervised work
- Taking part in a supervised or invigilated formative assessment
- The learner is being observed as part of a formative assessment.

TQT (Total Qualification Time)
'The number of notional hours which represents an estimate of the total amount of time that could reasonably be expected to be required, in order for a learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification.' The size of a qualification is determined by the TQT.

TQT is made up of the Guided Learning (GL) plus all other time taken in preparation, study or any other form of participation in education or training but not under the direct supervision of a lecturer, supervisor or tutor.

TQT is calculated at qualification level and not unit/component level.

Examples of unsupervised activities that could contribute to TQT include:

- Researching a topic and writing a report
- Watching an instructional online video at home/e-learning
- Watching a recorded webinar
- Compiling a portfolio in preparation for assessment
- Completing an unsupervised practical activity or work
- Rehearsing a presentation away from the classroom
- Practising skills unsupervised
- Requesting guidance via email – will not guarantee an immediate response.