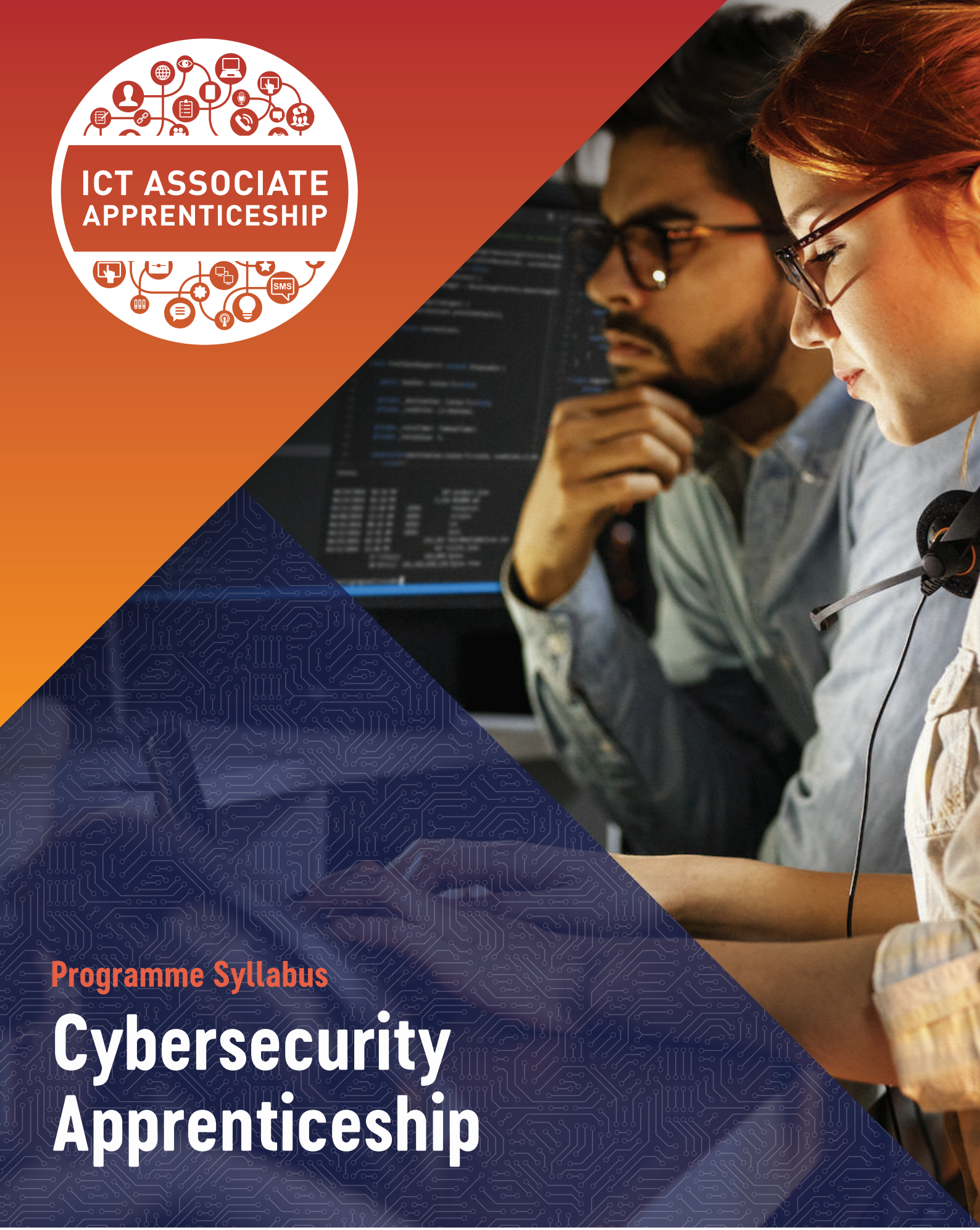
ICT ASSOCIATE APPRENTICESHIP



Programme Syllabus

Cybersecurity Apprenticeship

fit The Tech Talent Pipeline

GENERATION APPRENTICESHIP
www.apprenticeship.ie

Typical job roles in Cybersecurity include: Cloud Security Specialist, Penetration Tester, Junior IT Security Engineer, Risk Analyst, Security Sales Engineer, Cybersecurity Specialist, Information Security Assurance and Threat Analyst and Forensics and Incident Response Analyst.

1. Introduction

Apprenticeships are an exciting and proven way for employers to develop talent for their company and industry. Apprenticeships are designed by industry-led groups to support growth and competitiveness. Apprentices earn while they learn, and build valuable work-ready skills in a chosen occupation.

Apprenticeships open up exciting and rewarding careers, with learning grounded in the practical experience of undertaking an employment opportunity. Helping more people discover and develop their talents through training is at the heart of the national apprenticeship system. Assisting people to find opportunities through the acquisition of tech skills is at the heart of Fastrack into Information Technology's mission and we warmly welcome you to take part in this journey with our support and encouragement.

1.1 Programme Design

The Cybersecurity Apprenticeship is a two-year programme designed for those who have recently completed second-level education or mature learners who are seeking to retrain. It is a dual-education programme involving both college-based and workplace learning. This college-based learning is state-funded and apprentices receive a salary from their employer while on the programme. The programme provides apprentices with the theoretical and practical skills required to secure and retain employment within a work environment that has a cybersecurity focus. This programme utilises a number of CompTIA industry-recognised certifications to ensure programme content meets the rigors of training needs within contemporary cybersecurity workplace settings.

1.2 Stakeholders and Roles

Cybersecurity associates are charged with keeping data safe. In a digital society where everything is connected, it is critical that apprentices understand how networks are created, the flow of data and how it can be kept secure. Protecting data requires knowledge of the threat landscape, the tools and technologies to protect an organisation, security architecture, identity management, risk management and cryptography practices. Cybersecurity associates may further define their role as "Blue Team" or "Red Team" in orientation. Blue Team may be considered "defence" while Red Team may be considered "offence". All associates in this occupation work to achieve required security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil organisational requirements. They understand network topologies, cloud services, network administration and monitoring tools. They are able to give technical advice and guidance.

Cybersecurity apprentices will work in ICT industries researching, designing and testing security solutions. However, many will work in other sectors that require robust and safe systems to support their activity. Typical job roles include those of Cloud Security Specialist, Penetration Tester, Junior IT Security Engineer, Risk Analyst, Security Sales Engineer, Cybersecurity Specialist, Information Security, Threat Analyst, Forensics and Incident Response Analyst.

1.3 Governance

FIT is an industry-led not-for-profit organisation that develops and provides innovative education and training programmes. As Coordinating Provider, FIT is responsible for the operation and quality assurance of the programme. FIT works closely with its training delivery partners (ETBs), employers, and regulators (Quality and Qualifications Ireland, SOLAS, National Apprenticeship Office) to ensure that the ICT Apprenticeships meet the needs of all stakeholders.

2. Award Title, Level and QQI Certification

Successful completion of all modules on this programme leads to apprentice attainment of a Quality and Qualifications Ireland-accredited **Advanced Certificate in Cybersecurity**, which is placed at Level Six on the National Framework of Qualifications.

National Framework of Qualifications

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

2.1 Modular Components

The Cybersecurity apprenticeship programme integrates CompTIA technical certifications, City and Guild's components and Professional Recognition Award, transversal learning (e.g. communications, project management etc.) and workplace training into a holistic programme customised to the needs of a cybersecurity associate. The Advanced Certificate in Cybersecurity is a lifetime award. However, apprentice graduates may need to update their individual CompTIA certifications in the future.

Module	On / Off-the-job	Module Level Certification
Programme Induction	N/A	
GDPR (Data Protection)	N/A	
CompTIA IT Fundamentals	Off-the-Job	CompTIA
CompTIA Network+	Off-the-Job	CompTIA
CompTIA Security+	Off-the-Job	CompTIA
CompTIA Cyber Security Analyst CySA+	Off-the-Job	CompTIA
CompTIA Penetration Tester Pentest+	Off-the-Job	CompTIA
Professional Recognition Award (Information Technology)	Off-the-Job	City and Guilds
Effective Communications in Business	Off-the-Job	City and Guilds
Project Management	Off-the-Job	City and Guilds
Personal and Professional Development	Off-the-Job	City and Guilds
Capstone Project	Off-the-Job	
Applied Learning in the Workplace Year 1	On-the-Job	
Applied Learning in the Workplace Year 2	On-the-Job	

CompTIA

City & Guilds

3. Programme Access and Entry Requirements

FIT recruits candidates who express an interest in joining the programme by completing an online application form available on www.fit.ie. In the first instance, the application is subject to screening regarding the defined criteria noted below. Successful candidates will also be registered with SOLAS as the regulatory authority for the registration of apprentices in Ireland.

All candidates will be required to meet the specific entry requirements. Once the screening process has been finalised/completed, FIT will organise interviews between candidates and prospective host employers who will provide the mentored work placement opportunity to the candidate. The employer will select the applicant(s) to whom they will offer a role in their organisation as a full time employee for the duration of the programme. This decision is exclusively made by the employer and FIT has no role in influencing that decision-making process.

Since 2020, FIT has instigated several supports for candidates who may have additional support needs and who notify FIT of a disability at the candidate application stage. These supports range from assistance navigating the candidate application process to ongoing support during participation in the programme.

3.1 Specific Entry Requirements

Minimum candidate entry requirements are as follows:

- Must be 18 years or older,
- Will be required to complete an initial aptitude test,
- Must have achieved a passing grade (or O6/H7) in 5 or more subjects to include Maths and English (Ordinary Level) in the Irish Leaving Certificate,
- Must be eligible to participate in Further Education and Training programmes,
- Must be entitled to study and work in Ireland.

Equivalence may be decided through the Recognition of Prior Learning procedure for those who may not hold a suitable Leaving Certificate. In addition, those who have completed a FIT recognised Pre-Tech Apprenticeship programme will be able to furnish evidence of the same along with a copy of their Junior Certificate parchment/certificate.

Key candidate skills and attributes are as follows:

- Must be numerate and literate,
- Have good learning skills,
- Be interested in technology and customer service,
- Have the ability to absorb product knowledge,
- Be motivated and analytical,
- Possess good communication skills, pleasant personality, be determined to succeed,
- Have excellent interpersonal skills,
- Be able to work as a team member, be adaptable and flexible.

4. Programme Aims and Objectives

The Cybersecurity apprenticeship programme aims to enable the graduate apprentice to secure and retain employment in a computer security role. The apprentice should be able to combine technical, communications, project management and personal development skills to meet the requirements of an

employer and should be able to act autonomously or as part of a team as the occasion demands. The Cybersecurity apprenticeship programme involves a multi-layered approach to developing high-level computer networking and security skills. The initial layers, ICT Fundamentals and Network +, are not specific to computer security but cover the general terms, concepts, components and connectivity associated with computer systems and networks. These are scaffolding skills for a broad range of ICT roles in an organisation. The Security+ module marks the introduction to computer security technologies, principles and practices that are relevant to all organisations. The Security Analyst and Penetration Tester are specialist modules that equip the learner with the specific skills required to address cyber-attack and defence.

4.1 Specific Programme Objectives

Employers are increasingly aware of the need for a holistic approach to employee recruitment. It is important that cybersecurity associates can work effectively with management, colleagues and the public (where required). It is also important that they bring a structured approach to the execution of their duties and be able to play a leading role in their own personal and professional development. Transversal learning such as communications, project management, and personal development, are cross-disciplinary skills that have universal applicability and form an essential part of the objectives of this programme. In addition, apprentice development of a series of relevant technical skills and competencies is vital. With this in mind apprentices will be able to:

- Explain why Cybersecurity matters – the importance to business and society.
- Describe concepts such as security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard and the relationship between these concepts in the context of risk and harm.
- Explain what assurance means, what methods are used to achieve assurance and the distinction between “trustworthy” and “trusted”.
- Discuss the considerations for building a security case, building security objectives with reasoned justification in representative business scenarios.
- Identify the fundamental building blocks and typical architectures of ICT infrastructures and list some common vulnerabilities in computer networks and systems.
- Give examples of the main attack techniques and sources of threat and explain how these techniques combine with motive and opportunity to become a threat.
- Describe ways to defend against attack techniques.
- Discuss technical and ethical standards and the key features of applicable national and international laws and regulations pertaining to data security.
- Describe how to apply relevant techniques for horizon scanning, including use of recognised sources of threat intelligence.
- Analyse the significance of identified trends in cybersecurity and the value and risks associated with this analysis.
- Discover system vulnerabilities through research and practical exploration.
- Analyse and evaluate security threats and hazards to systems, processes and services.
- Demonstrate the use of relevant research of external sources of threat intelligence or advice (e.g. OWASP), combining different sources to create an enriched view.
- Undertake a security risk assessment for a system without direct supervision and propose remediation advice in the context of the organisation.

- Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe the threats, vulnerabilities or risks mitigated and identify any residual areas for concern.
- Develop without supervision, a security case which comprises documented security objectives, threats, attack techniques and possible mitigations or security controls (e.g. technical, implementation, policy or process).
- Implement organisational policies and standards for information and cybersecurity within their scope of influence and responsibility.
- Operate in accordance with service level agreements or employer-defined performance targets.
- Define the organisational implications of anticipated future trends in cybersecurity. CompTIA A + and CompTIA Network +.

5. Programme Structure

The Cybersecurity Apprenticeship programme is presented in four semesters that chart apprentice growth and progress through the programme.

Semester 1: Laying the Foundation

Apprentices will receive a 'deep dive' of technical and transversal learning in preparation for entry to the workplace. As the title suggests, the purpose of this semester is to "lay the foundation" for the technical knowledge that learners will rely on in Semester 2. It will also help apprentices "find their feet" and introduce them to fellow apprentices and tutors.

Semester 2: Introducing the Workplace

In Semester 2, the off-the-job training/activity combines with time spent in the workplace setting. Apprentices will undertake additional workplace practice to increase their knowledge and skills. The learning undertaken in the workplace will be guided by the tasks outlined in the module "Application of Skills in the Workplace Year 1". The broader purpose of this semester is to integrate apprentices fully into the workplace setting, to introduce the apprentice to their work teams and mentors, and to start applying acquired knowledge and skills. This stage builds on the technical learning undertaken in Semester 1. Off-the-job training activity will enable learners to "re-group" in a familiar setting, share workplace experiences and discuss technical matters with tutors.

Semester 3: Consolidation

Semester 3 continues the model of off-the-job training/activity and work placement. The difference in this semester is that many off-the-job modules have concluded, allowing apprentices to actively contribute to work teams enabling them to focus on consolidating theoretical learning by continuing to apply skills in the workplace. In addition, as in Semester 2, the off-the-job activity will provide a continuing opportunity for engaging with peers and tutors.

Semester 4: Preparation for Autonomy

The final semester will assist apprentices in adapting to full-time employment with more autonomy. Some time will still be allocated to engage with peer groups and tutors. During this semester, the apprentice's future path will become more apparent. It may be that the employer indicates that the apprentice will be offered a role with them upon completion of the apprenticeship. If not, the apprentice will be facilitated to seek alternate employment or further training at the end of the programme. This semester provides the opportunity to address issues of further education or supports to secure alternate employment where necessary.

5.1 Specific On and Off-the-Job Timings

Depending upon the noted employer need, the programme may run on either a day release or block release structure to accommodate the required off-the-job modules/elements. The format of particular cohort instance starts will be notified in advance to apprentices and all stakeholders.

Typical Day Release Arrangements*

Semester 1	26 Weeks	Full time off-the-job training Monday-Friday
Semester 2	26 Weeks	Monday and Tuesday day release off-the-job training each week *Remainder of time spent full time in the workplace*
Semester 3	26 Weeks	Monday and Tuesday day release off-the-job training each week *Remainder of time spent full time in the workplace*
Semester 4	26 Weeks	Monday day release off-the-job training *Remainder of time spent full time in the workplace*

** May be subject to change dependant upon employer needs.*

Typical Block Release Arrangements

Block release arrangement timings may vary from intake to intake following discussion with employers and in consultation with off-the-job delivery partner, the ETBs. However, confirmed block release arrangements will ensure completion of the required total learning hours in both on and off-the-job study as these timings form critical requirements of the programme validation.

6. Indicative Programme Content Summary

The indicative content that forms this programme builds upon increasing complexity from the first to final modules. Early programme modules are targeted towards an NFQ level 5 and Level 6 standard. This approach allows for an accessible learning experience for those coming new to ICT to understand fundamental topics, technologies and their application while also building their knowledge and skills throughout the programme. The indicative content noted below comprises a brief snapshot of content relating to constituent programme modules. A complete outline of module-specific learning outcomes and aligned indicative content is available by request. Alternatively, FIT is always open to discussing specific programme aspects or where future enhancements can be made.

M01 **CompTIA IT Fundamentals**

This foundational module intends to establish a common base of understanding among apprentices. It discusses basic computer components, how to set up a workstation, install software, establish basic network connectivity, identify compatibility issues, identify/prevent basic security risks, and safety and preventative maintenance of computers.

M02 **CompTIA Network+**

This module addresses the knowledge and skills required to troubleshoot, configure, and manage common network devices; establish basic network connectivity; understand and maintain network documentation; identify network limitations and weaknesses; and implement network security, standards, and protocols. Apprentices will develop a basic understanding of enterprise technologies, including cloud and virtualization technologies.

M03 **Effective Communications in Business** (City and Guilds Unit 401)

The purpose of this module is to provide apprentices with an understanding of the importance of effective communication (written, verbal and non-verbal) in a business environment. Also, apprentices will understand why effective communication is critical for businesses and will be able to recommend different types of communication methods suitable for specific purposes.

M04 **CompTIA Security+**

This module addresses the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. Apprentices will perform these tasks to support the principles of confidentiality, integrity, and availability.

M05 **CompTIA Cybersecurity Analyst CySA+**

This module addresses the knowledge and skills required to configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats, and risks to an organisation with the end goal of securing and protecting applications and systems within an organisation.

M06 **Project Management** (City and Guilds Unit 400)

This module aims to provide apprentices with an understanding of project management principles and how projects are set up. Apprentices will gain an understanding of how to mitigate for risks and develop their skills in using management tools to monitor and review projects.

M07 **Applied Learning in the Workplace Year 1**

Within the context of a supported work environment, this module aims to provide apprentices with an opportunity to demonstrate and document their application of learning in a workplace setting, relating to both occupationally specific technical and transversal skills acquisition. The focus will be on the application of IT networking skills and transversal skills.

M08 **CompTIA Penetration Tester Pentest+**

This module addresses the knowledge and skills required to plan and scope an assessment, understand legal and compliance requirements, perform vulnerability scanning and penetration testing using appropriate tools and techniques, and analyse and report investigation results.

M09 **Personal and Professional Development** (City and Guilds Unit 403)

This module aims to provide apprentices with an understanding of the different methods and resources available to help them plan for their personal and professional development. They will learn how to identify factors that may affect targets or goals, prioritise actions and understand how feedback from others can be utilised to aid their development and career progression. As a result, they will be able to develop a plan which can either be used to progress to a course of study or as a tool for their future/ current career path.

M10 **Applied Learning in the Workplace Year 2**

Within the context of a supported work environment, this module aims to provide apprentices with an opportunity to demonstrate and document their application of learning in a workplace setting, relating to both occupationally specific technical and transversal skills acquisition. The focus will be on the application of IT security skills and transversal skills.

M11 **GDPR General Data Protection Regulations** (non-accredited)

Data Protection Regulations in a European context called the General Data Protection Regulation (GDPR) came into effect across Europe in May 2018. At its core, GDPR is a set of rules designed to give EU citizens more control over their personal data. In addition, it aims to simplify the regulatory environment for businesses so both citizens and businesses in the European Union can fully benefit from the digital economy. However, information gets lost, stolen or otherwise released into the hands of people who were never intended to see it -- and those people often have malicious intent. Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so. Cybersecurity Specialists are at the forefront of data protection and they need to be aware of the provisions of the GDPR. This short module provides insight into robust personal data management practices and an overview of the GDPR.

M12 **Professional Recognition Award** (City and Guilds)

The C&G Professional Recognition Awards are designed to recognise experiential learning in the workplace. Through completion of a portfolio, apprentices will evidence that they meet six standards including:

Standard 1 Commitment to professional standards.
Standard 2 Communication and information management.
Standard 3 Leadership.
Standard 4 Professional development.
Standard 5 Working with others.
Standard 6 Managing customer relationships.

M13 **Capstone Project**

The Capstone Project is an assignment that draws on the classroom and work-based learning to form a holistic assessment. Apprentices will undertake an exercise based on Red Team (offensive) and Blue Team (defensive) roles. They will be assessed on the write-up of the exercise.

7. Assessment of Learning

Programme elements are assessed in different ways. During the completion of off-the-job modules, apprentices will undertake a series of assessment tasks for each module that demonstrate apprentice attainment of the required minimum standards. Apprentices complete assessments in a controlled tutor-invigilated environment that is time-bound against set and diverse assignment briefs. Typically assessment aligned to a particular module is completed within the final days of the delivery of a particular module. As apprentices progress through the programme, they will have the opportunity to complete some CompTIA certification, which typically necessitates attendance at a defined testing centre location. Workplace learning is monitored through apprentices providing written responses regarding the completion of defined and relevant workplace tasks of both a hard technical nature and concerning the application of transversal skills. These responses are monitored by the Workplace Learning Officer, reviewed by the Workplace Mentor and assessed by a FIT-appointed Workplace ICT Assessor.

8. Contact Information / National Availability

The programme may commence at any point during the calendar year, depending on a wide range of factors affecting delivery and placement. Programmes typically comprise classes of 15-18 apprentices. The frequency of programmes and the selected locations will be related to regional demand from employers for the Cybersecurity Apprenticeship programme.

FIT Contact Information
Phone: 01 8825570 **Email:** info@fit.ie **Web:** www.fit.ie

Version 2.0

fit The Tech Talent Pipeline

GENERATION APPRENTICESHIP
www.apprenticeship.ie

SOLAS learning works®

etbi
Education and Training Boards Ireland
Boird Oideachais agus Oiliúna Éireann