ICT ASSOCIATE APPRENTICESHIP

Programme Syllabus

Cybersecurity Apprenticeship

An innovative apprenticeship that combines cybersecurity and operating system management skills with contemporary application of generative AI tooling, networking technologies, threat response and risk analysis techniques, project management, and more.

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, Digital Forensics, and Incident Response Analyst.

1. Introduction

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

Completing the apprenticeship journey opens up exciting and rewarding careers for motivated learners with an interest in cybersecurity. This exposure to a learning environment, grounded in the practical experience associated with a workplace, is the heart of the national apprenticeship system and helps learners discover and develop their talents to the fullest extent. Our mission at Fastrack into Information Technology, then, is to assist people in finding opportunities through the acquisition of tech skills in the face of rapid technological changes. We warmly invite you to take part in this journey, where you will be accompanied by our support and encouragement at all times.

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 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. Apprentices get the opportunity to achieve industry-recognised certifications from CompTIA, providing the rigorous training required to excel in the dynamic professional world of cybersecurity. Recently, FIT concluded the first formal large-scale review of this programme, culminating in a modified programme targeted toward meeting contemporary business needs.

1.2 Impact of AI on Cybersecurity

The functionality and usefulness of various generative AI-based tools and associated technologies have increasingly proved their worth to small businesses, public services providers, and large multi-national organisations alike. AI technologies play a crucial role in cybersecurity by enhancing threat detection, prediction, and response capabilities. AI tools can analyse vast amounts of data to identify patterns and anomalies, predict potential cyber threats, automate certain security tasks, and respond to real-time incidents. This helps to bolster defences, mitigate risks, and protect against evolving cyber threats more effectively. Future apprentices will increasingly utilise these technologies in their day-to-day activities. As such, demystifying key AI concepts and awareness of the real-world application of generative AI tooling is essential to provide a solid base for apprentices commencing this apprenticeship programme.

All candidates who apply to this programme will be provided access to a self-paced, online learning path developed by IBM that provides an accessible and introductory understanding to AI ethics and practical prompting strategies. In addition, during the completion of the programme, apprentices will utilise generative AI tools within network and security environments during their off-the-job programme elements, providing insight into how generative AI tools enable security teams to observe, analyse, detect, and block suspicious artefacts traversing a network.

It is important to note that the design of this programme does not rely on a narrow variety of threat detection skills. **This programme aims to holistically develop abilities crucial for cybersecurity specialists across various contemporary themes, which have increasing relevance and currency for employers offering ICT services, as well as those who use, manage, and maintain large-scale ICT systems.**

1.3 Stakeholders and Roles

Cybersecurity specialists 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 they 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 also specialise in "Blue Team" or "Red Team" roles, corresponding to "defensive" or "offensive" activities, respectively. All associates in this occupation work to achieve required security outcomes in legal and regulatory contexts 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 regular functioning. Typical employment opportunities in this field are diverse and include: **Cloud Security Specialist, Penetration Tester, Junior IT Security Engineer, Risk Analyst, Security Sales Engineer, Cybersecurity Specialist, Information Security, Threat Analyst, Digital Forensics,** and **Incident Response Analyst**.

1.4 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 operational and quality assurance aspects of the programme. FIT works closely with its training delivery partners (ETBs), employers, and regulators (namely: Quality and Qualifications Ireland, SOLAS, and the 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 results in the 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

APPROVED QQI AWARD PROVIDER

2.1 Modular Components

The Advanced Certificate in Cybersecurity is a lifetime award that also affords apprentices the opportunity to achieve valuable industry certifications. Apprentices will be made aware of the need to keep these CompTIA certifications up to date post-programme completion, and throughout their professional careers.

Module	Course Type	FET Credits	Module Level Certification
Programme Induction	Off-the-Job	0	
GDPR (Data Protection)	Off-the-Job	0	
Networking Fundamentals	Off-the-Job	15	
Cybersecurity in Operating Systems: Linux & Windows	Off-the-Job	15	
Intermediate Network Management	Off-the-Job	35	CompTIA Network+
Applied Cybersecurity: Threat Response & Secure Architecture	Off-the-Job	30	CompTIA Security+
Cybersecurity Operations: Risk Analysis & Artificial Intelligence	Off-the-Job	30	CompTIA Cybersecurity Analyst (CySA+)
Project Management & Communications	Off-the-Job	10	
Capstone Project	Off-the-Job	15	
Applied Learning in the Workplace: Year 1	On-the-Job	25	
Applied Learning in the Workplace: Year 2	On-the-Job	25	

3. Programme Access and Entry Requirements

FIT recruits candidates who express an interest in joining the programme by completing an online application form, available at www.fit.ie. Initially, the application is screened with respect to basic eligibility requirements 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 completed, FIT will organise interviews between candidates and prospective host employers who will then provide the mentored work placement environment. The employer will select the applicant(s) to whom they will offer a role in their organisation as full time employee for the duration of the programme. This decision is made exclusively by the employer and FIT has no role in this candidate selection process.

Since 2018, FIT has made available several supports for candidates who may have additional learning needs. Candidates with such requirements or disabilities are given the opportunity to make this known to FIT from the start of the application process. These supports range from assistance in navigating the candidate application process to ongoing support during participation in the programme, including advice on reasonable accommodations.

3.1 Specific Entry Requirements

Minimum candidate entry requirements are as follows. A successful candidate:

- 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, including Mathematics and English (both at Ordinary Level or above), in the Irish Leaving Certificate;
- Must be eligible to participate in Further Education and Training programmes; and
- Must be entitled to study and work in Ireland.

The Recognition of Prior Learning procedure may be employed in determining equivalence to the above requirements for those candidates without a suitable Leaving Certificate qualification. Additionally, those who have completed a FIT recognised Pre-Tech Apprenticeship programme will have the opportunity to furnish evidence of the same along with a copy of their Junior Certificate transcript as part of this process.

Key candidate skills and attributes are as follows. A successful candidate 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, a pleasant personality, and be determined to succeed;
- Have excellent interpersonal skills;
- Be able to work as a team member; and
- 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 digital security role. Candidates accepted into the programme 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 takes a multi-layered approach to developing high-level computer networking and security skills. The initial modules are not specific to cybersecurity but cover the general terms, concepts, components, and connectivity issues associated with various computer systems and networks. These are scaffolding skills for a broad range of ICT roles within an organisation. Later in the programme, the Applied Cybersecurity module introduces cybersecurity technologies, principles, and practices that are relevant to all organisations, while the Cybersecurity Operations module will equip the apprentice with the skills required to address cyber-attacks and defend themselves in a critical environment.

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 general public (where applicable). It is also important that they bring a structured approach to the execution of their duties and are able to play a leading role in their own personal and professional development. Transversal learning activities 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 is important for businesses, as well as wider society more broadly;
- 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, establishing 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 threat sources to ICT systems, explaining how these techniques become threats with the presence of motive and opportunity;
- Describe ways to defend against attack techniques;
- Discuss technical and ethical standards, as well as the key features of applicable laws and regulations (from national and international sources), 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, along with the value and risks associated with this analysis;

- Discover system vulnerabilities through research and practical exploration;
- Using generative artificial intelligence/machine learning solutions, analyse and evaluate security threats and hazards to systems, processes, and services;
- Demonstrate the ability to perform relevant research, using external sources of threat intelligence and best practices (e.g. OWASP), to establish a detailed picture of cybersecurity threats;
- Undertake a security risk assessment for a system, without direct supervision, and propose remediation advice in an organisational context;
- 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 (under common headings such as 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; and
- Define the organisational implications of anticipated future trends in cybersecurity.

5. Programme Structure

The Cybersecurity Apprenticeship programme is delivered across four semesters. The titles of these semesters correspond with specific milestones necessary for meaningful apprentice progress.

- **Semester 1:** Laying the Foundation.
- **Semester 2:** Introducing the Workplace.
- **Semester 3:** Consolidation.
- **Semester 4:** Preparation for Autonomy.

The table on Page 8 details typical on-the-job (WORKPLACE) and off-the-job (COLLEGE) timings for this two-year, full-time apprenticeship programme. Attendance for the duration of each full day of training, either in college or the workplace, is mandatory.

The college-based training aspect of this programme is usually delivered in person. Candidates are notified of specific arrangements once they prepare to commence employment with their apprenticeship employer. In practice, apprentices attend an Education and Training Board facility for college-based training. These facilities are based throughout the Republic of Ireland and offer apprentices a high-quality training experience. FIT endeavours, where feasible, to align the geographic location of college-based training with the location of an employer's business operations. However, this is not possible in all instances, and so candidates must be willing to make arrangements to travel in order to attend specified training locations.

Subject to accreditor approval, in a small number of intake instances each year college-based training elements may be delivered via a blended approach to instruction. In such cases, apprentices conduct training sessions from home, or their place of work, via a virtual classroom. However, some in-person attendance will still be required.

5. Programme Structure (continued)

Typical Weekly Delivery Schedule Year 1 (Semesters 1 & 2)

Week Numbers	*Location*	*Days*
1 – 3	**Workplace**	**Monday – Friday**
4 – 17	College	Monday – Friday
18 – 33	**Workplace**	**Monday – Friday**
34 – 43	College	Monday – Friday
44 – 52	**Workplace**	**Monday – Friday**

Typical Weekly Delivery Schedule Year 2 (Semesters 3 & 4)

Week Numbers	*Location*	*Days*
53 – 60	College	Monday – Friday
61 – 78	**Workplace**	**Tuesday – Friday**
79 – 80	College	Monday – Friday
81 – 104	**Workplace**	**Monday – Friday**

Occasionally, where a single employer may aim to recruit an entire participating cohort of 14+ apprentices, there is the possibility of modifying these timings in accordance with employer preferences and requirements. All programmes, regardless of specific scheduling adjustments, will complete the total required learning hours for on- and off-the-job training periods.

6. Indicative Programme Content Summary

The indicative content noted below comprises a brief snapshot of key subject matter covered in the programme's constituent modules. A complete outline of module-specific learning outcomes and aligned indicative content is available on request. As part of FIT's commitment to transparency and dynamic service provision, feedback relating to specific aspects of the programme—including possibilities for future enhancements—is always welcome.

CS-TA-001 **Networking Fundamentals**

This module introduces apprentices to the basics of computer networking, without assuming any prior knowledge of the subject. It begins with an overview of the OSI and TCP/IP models, as well as the history of their development, equipping apprentices with a useful conceptual framework by which the technologies and protocols of networking can be easily understood and analysed. These technologies are then explored in both practical and theoretical terms, as common networking set-ups are presented via interactive demonstrations. By the end of the module, apprentices will put these ideas into practice by mapping out simple Local Area Networks (LANs).

CS-TA-002 **Cybersecurity in Operating Systems: Linux & Windows**

To contextualise the basic principles of cybersecurity an understanding of how operating systems work, in both broad and specific terms, is essential. This module provides that context by, initially, outlining the structure of Windows and Linux based operating systems, before clarifying their role in establishing secure ICT systems. Building on work done in the previous module, apprentices will be exposed to a variety of good practices when setting up and maintaining operating systems within an overall ICT set-up. Practical tools such as *Wireshark*, and command line interfaces, will be demonstrated to apprentices to make these principles more tangible and understandable.

CS-TA-003 **Intermediate Network Management**

Where *Networking Fundamentals* gave apprentices a relatively high-level overview of networking principles, this module goes into detail on the nuts-and-bolts of networking in common, real-world scenarios. To begin, apprentices will gain an appreciation for the need to maintain networked systems. To assist with this, apprentices will be shown how to accurately implement appropriate software and hardware components to ensure that a specific network is as efficient as possible. As with the previous modules, real-world impacts will be a constant guiding focus: budgetary constraints and their effects on network administration, for instance, will be discussed and analysed. Apprentices will also get the opportunity to utilise forensic analysis tools to identify and mitigate potential cybersecurity threats, emphasising the need for "robustness" in an organisation's networking infrastructure.

CS-TA-004 **Applied Cybersecurity: Threat Response & Secure Architecture**

Having been exposed to foundational principles of cybersecurity, this module shows apprentices strategies for responding to cybersecurity threats in the wild. This response is both proactive and reactive, as apprentices will also learn how to implement ICT systems that are secure against the most common types of cyber-threats. Following on from the previous module, apprentices will gain an appreciation for the need to make ICT systems policies comprehensible in plain terms to the average end user—a system is only secure if its users know how to use it safely and report any suspicious behaviour. Apprentices will see how different environments, such as cloud computing set-ups, can affect security considerations and will gain hands-on experience of using network intrusion detection systems. After the initial focus on the types of cyber-threats, apprentices will be introduced to the theory behind cybersecurity tools that keep these threats at bay.

CS-TA-005 **Cybersecurity Operations: Risk Analysis & Artificial Intelligence**

Responding appropriately to these risks is critically important and so apprentices will learn about different incident response activities, as well as the ways in which cyber-threats can be hunted and mitigated. Given the close link between modern cybersecurity applications (such as antivirus software) and Artificial Intelligence (AI), apprentices will be provided with a broad overview of the fundamentals of AI. In keeping with the Apprenticeship Programme's practical focus, apprentices will get hands-on experience with AI tools to illustrate, for example, how bad (or poorly defined) inputs can result in bad outputs. The relevance, here, to cybersecurity will be made clear: AI tools are only useful if they are used correctly and in appropriate contexts. Apprentices will also explore risk in the context of AI, given the need to protect sensitive company data from misuse by AI technologies.

CS-TA-006 **Project Management & Communications**

While it is important to have deep technical knowledge of networking and cybersecurity to become a successful cybersecurity professional, that success is limited if apprentices are unable to communicate clearly or understand how to efficiently manage large projects. Beginning with the common approaches to project management, this module answers many questions apprentices may have about policies related to teamwork and project progression in light of their first-hand experience of the workplace. Not only will apprentices learn why organisations use different project management strategies, they will also get the chance to put one into practice for themselves. Using different monitoring and evaluation techniques, apprentices will learn how to successfully introduce a project and see it through to completion with the minimum of disruption.

CS-TA-007 **Capstone Project**

The purpose of this module is to provide apprentices with a "feather in their cap" in the form of an impressive showcase project. All the hard work throughout the programme has paid off and apprentices are now more than able to put together a project that would stand out on any portfolio. Tutors will help apprentices choose a project that is right for them, and their career aspirations, from a list of key cybersecurity domains pre-approved by FIT, including: Penetration Testing, Risk Management, and Cloud Security. The parameters and initial scenario of these projects will be set by the tutor, who is best placed to understand the strengths and interests of their class group. While tutors will assist apprentices in responding to queries related to their project work, much of this work will be self-directed. This gives apprentices the opportunity to put into practice both insights gleaned from experience in the workplace and technical knowledge covered in the previous modules.

CS-TA-008 **Applied Learning in the Workplace: Year 1**

Throughout their time in the workplace, apprentices will track their progress and implementation of specific technical knowledge via the logbook introduced in this module. Additionally, this logbook will track their use of non-technical skills, such as communication best practices explored in the previous module. This emphasis on both technical and non-technical skills is a crucial component of the Apprenticeship Programme: a successful graduate will know how to accurately perform technical tasks and will be able to report on their work in a clear, professional manner. The reflective exercises in the logbook ensure that this dual focus is emphasised at all times, while also providing apprentices with a model for achieving personal and professional development in their future careers. To assist in their completion of the logbook, the apprentice will liaise closely with their appointed Workplace Assessor and Workplace Mentor.

CS-TA-009 **Applied Learning in the Workplace: Year 2**

As with the previous semester, this module utilises the logbook as a tool to reinforce the focus on technical and non-technical skills alike. While no sensitive company data or intellectual property will be recorded in the logbook, apprentices will find that their entries will increase in complexity; especially in terms of applied technical skills. This increase in complexity will stand as testament to the apprentice: the progress in their technical expertise in the short time span of just a few months is evidence of their hard work and diligence.

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, proctored environment that is time-bound against specific assignment briefs. Typically, assessment of a particular module is completed within the final days of the delivery of that module. As apprentices progress through the programme, they will have the opportunity to complete some CompTIA certifications, which typically necessitates attendance at a defined testing centre location. Workplace learning is monitored through the use of the logbook, where apprentices provide detailed written entries describing relevant workplace tasks of a technical nature. Entries demonstrating examples of apprentices employing transversal skills in the workplace are also required. These activities 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 14+ 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

fit The Tech Talent Pipeline

GENERATION APPRENTICESHIP
www.apprenticeship.ie

SOLAS learning works®

etbi
Education and Training Boards Ireland
Boird Oideachais agus Oiliúna Éireann