LEVEL 4 CYBER SECURITY TECHNOLOGIST

There is nothing standard about the new apprenticeship Standards!

In 2017 modern apprenticeships underwent a major overhaul. Apprenticeships now represent the very best in vocational Further Education programmes and benefit the widest range of employees and employers for new career starts, upskilling for progression or changes in career direction.

Programme Overview:

There are two separate pathways available in this apprenticeship - Technologist and Risk Analyst.

Who is the Technologist for?

The **Technologist** will mitigate cyber threats, hazards and risks to protect an organisation's systems and people. A technical focus includes security, design, architecture, testing, investigation and response. Roles include:

- Cyber Operations Manager
- Security Architect, Engineer or Analyst
- Cyber Security Specialist
- Information Security Assurance and Threat Analyst
- Forensics and Incident Response Analyst
- Information Security Analyst, Auditor, Administrator or Officer

Who is the Risk Analyst for?

The **Risk Analyst** focusses on operational risk, governance and compliance. Roles include:

- Governance and Compliance Analyst
- Risk Analyst, Intelligence Researcher

Both pathways 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 knowledge of information security to deliver solutions to meet the organisation's requirements.

Entry Requirements:

Entry requirements exist for all funded Further Education programmes. These ensure the value, gain and success of the programme. The ATP will conduct the processes with employers and prospective apprentices to determine correct funding eligibility.

Job role eligibility (known as Competency Role Map):

The job role must contain opportunity for an apprentice to practice the content set out in the apprenticeship Standard to achieve vocational competency. Apprentices must have the opportunity to practice the knowledge taught in training sessions in order to convert new knowledge in to sustainable skills applied in the workplace.

Each apprenticeship requires a portfolio of evidence this will showcase the apprentice's work and will be reviewed by the apprenticeship assessment organisation to determine how well new knowledge has been successfully utilised vocationally. If a job role is close to the eligibility criteria we will consult with employers to see if adjustments can be made to ensure criteria is met.

Initial Assessment of existing knowledge and skills:

A prospective apprentice must stand to gain significant knowledge and skills from an apprenticeship. If the apprenticeship is too advanced for them or if they already know much of the knowledge and skills the apprenticeship would provide then they may not be eligible for the funding.

The ATP will review existing qualifications, knowledge and skills to determine if the prospective apprentice will benefit from the proposed apprenticeship such that it meets the funding criteria. In most instances this is very straightforward, however in some instances funding can be specially authorised for reduction in order to fund the parts of an apprenticeship that would be relevant. The ATP will provide the assessment for these possibilities.

The Level 4 Cyber Security Technologist apprenticeship is highly technical. Whilst employers can select their own entry criteria, prospective apprentices should have achieved at least 5 GCSEs including English and Mathematics and hold a minimum of 120 UCAS points, or equivalent in relevant subject areas.

In many cases this type of apprenticeship can demand a higher capability of English and maths than is taught at GCSE or A-Level. For example, advanced report writing, budgeting, complex structured explanations and/or advanced formulae and statistics. The ATP will provide both functional and advanced English and maths diagnostics and teaching to ensure each apprentice is fully supported in these areas.

Programme Duration:

This apprenticeship is delivered over 24 months for full-time employees. For part-time employees the term may be extended depending on the contracted hours.

Standard Delivery Model:

Apprenticeship training is delivered through a blend of weekly live web-based classrooms and regular face-to-face mentoring sessions that are held on a one-to-one basis in the workplace.

These live classrooms are held through Microsoft Teams. This software provides the full suite of educational tools including everything you would find in a conventional classroom and more e.g. live open interactions, private breakout rooms, note and question queues and interactive illustration boards. We can also use movie green screen technology for lesson illustrations.

A full timetable for the training, mentoring, exams and assessments is provided at the outset. Progress is reviewed at 12-week intervals in a meeting between the mentor, apprentice and employer (typically the apprentice's line manager).

Employers and apprentices have full visibility of progress in real-time by accessing the e-portfolio system, alternatively regular updates can be provided by other means if preferred.

End Point Assessment (EPA):

Aside from qualifications that can be obtained by doing an apprenticeship, the most important and valuable goal is what has been achieved during the programme.

Successful apprentices will obtain a Pass, Merit or Distinction in their apprenticeship. The way a Pass, Merit or Distinction is determined is at a stage called End Point Assessment which takes place once all the leaning has been completed. Like all examinations, a mock will take place before the final assessment.

Once all components of the apprenticeship have been achieved including the mock, a final review is conducted to ensure everything has been covered, this is called gateway. Then the apprentice will undergo their EPA.

The EPA for this programme consists of:

1. Portfolio of Evidence demonstrating work on 6-8 projects covering all the criteria
2. Employer Reference built over the course of the apprenticeship during the 12 week reviews, covering all the standard criteria
3. Synoptic Project, a business project completed in the final stages of the apprenticeship (this can sometimes include a virtual lab where appropriate), taking between 10-40 hours over a maximum of 2 weeks
4. A structured interview with the assessors exploring the project, portfolio of evidence and employer reference

Programme Structure:

Technical Competencies:

Threats, hazards, risks and intelligence:

- Combines research and practical exploration to determine system vulnerabilities
- Analyses and evaluates security threats and hazards to systems, services or processes
- Utilises sources of threat intelligence or advice
- Understands common attack techniques and recommends how to defend against them
- Demonstrates use of relevant external sources of vulnerability (e.g. OWASP)
- Autonomously undertakes security risk assessments for a simple systems and provides basic remediation advice
- Identifies anomalies in network data structures and behaviours

Developing and using a security case:

- Sources and analyses a security case and describes what threats, vulnerabilities and risks are mitigated and identifies residual areas of concern
- Autonomously develops a simple security case expressing security objectives and threats, then for each identified attack technique determine mitigation or security controls which include technical, implementation and policy or process

Organisational Context:

- Follows organisational policies and standards for information and cyber security
- Operates according to service level agreements or employer defined performance targets.

Future trends:

- Investigates different views and sources of future trends in a relevant technology area and can describe, with supporting reasoning, the relevance to the organisation.

Underpinning Skills, Attitudes and Behaviours:

- Logical and creative thinking
- Analysis and problem solving
- Personal responsibility and independent working
- Personal initiative
- Thorough and organised approach
- Ability to work with colleagues and clients
- Communicate effectively in a variety of situations
- Maintain productive, professional and secure working environment

Qualifications and Certifications:

Knowledge Module 1 (Core Elements):

Cyber Security Introduction

AND EITHER

Technologist pathway:

Knowledge Module 2:

Network and Digital Communications Theory

Knowledge Module 3:

Security Case Development and Design Good Practice

Knowledge module 4:

Security Technology Building Blocks

Knowledge Module 5:

Employment of Cryptography

OR

Risk Analyst pathway:

Knowledge Module 6:

Risk Assessment

Knowledge Module 7:

Governance, Organisation, Law, Regulation & Standards

Core Elements:

Technical Knowledge and Understanding:

Why Cyber Security matters: the importance of security to business and society

Basic security theory: security, identity, confidentiality, integrity, availability, threat, vulnerability, risk and hazard

Basic security assurance: deriving security objectives with reasoned justification in a representative business scenario. Understanding security assurance concepts and practices

Applying security to ICT infrastructure: describes fundamental building blocks and architectures and identifies common network and system vulnerabilities

Attack techniques and threat sources: understands the threat landscape and how common attack techniques combine with motive and opportunity to become a threat

Cyber Defence: Understand the asymmetric nature of Cyber Security and how to protect our information assets from threats

Relevant laws and ethics: understands security standards and regulations and their impact within industry. Understands common features of criminal, civil UK and international law.

Current threat landscape & Future trends: can describe and deploy relevant techniques for horizon scanning, utilising recognised sources of threat intelligence

Technologist pathway:

Technical Competencies:

Network building: design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to includes servers, hubs, switches, routers and user devices to a given design requirement without supervision. Provide evidence that the system meets the design requirement.

Prepare a security case: analyse functional and non-functional security requirements that may be presented in a security case against other design requirements. E.g. usability, cost, size, weight, power, heat, supportability etc. provided for a particular system or product. Identify conflicting requirements and propose, with reasoning, resolutions through appropriate trade-offs.

Build a secure network: design and build a simple system (can be at enterprise, network or application layer) in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case.

Select and configure relevant types of common security hardware and software components to implement a given security policy.

Design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the system.

Technical Knowledge and Understanding:

Understands network basics: data, protocols and how they interrelate; main routing protocols; main factors affecting network performance including typical failure modes in protocols and approaches to error control

Security cases: can describe what good design practices are; understands common security architectures; aware of reputable security architectures that incorporate hardware and software components. Knows sources of architecture patterns and guidance.

Understand how to build security cases including context, and threats, justifying selected mitigations and security controls with reasoning, and recognising the dynamic and adaptable nature of threats. Understands how cyber security technology components are typically deployed in networks and systems to provide security functionality in hardware and software.

Understands the basics of cryptography, can describe main techniques, significance of key management and legal issues.

Risk Analyst pathway:

Technical Competencies:

Cyber security risk assessment: conduct a cyber risk assessment against an external, market recognised cyber security standard, using a recognised risk assessment methodology. Identify threats relevant to a specific organisation and/or sector.

Information security policy and process: develop an information security policy or process to address an identified risk.

Develop an information security policy within a defined scope to take account of a minimum of one law or regulation relevant to cyber security.

Audit and assurance: take an active part in a security audit against a recognised standard, undertake a gap analysis and make recommendations for remediation.

Incident response and business continuity: Prepare an incident response plan for approval, within organisational governance arrangements for incident response.

Prepare a business continuity plan for approval, within the organisational governance arrangements for business continuity.

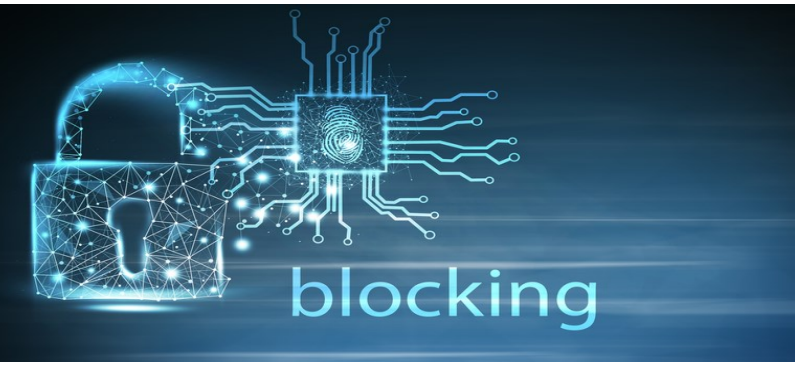
Cyber security culture in an organisation: Assess security culture using a recognised approach. Design and implement a simple 'security awareness' campaign to address a specific aspect of a security culture

Technical Knowledge and Understanding:

Understands risk: assessment methodologies and approaches to risk treatment. Can identify vulnerabilities in organisational and security management systems, understands the threat intelligence lifecycle, can describe different approaches to risk treatment.

Understand the role of the risk owner and the contrast with other stakeholders.

Knowledge of legal, regulatory and ethical standards relevant to cyber security: governance, organisational structure, roles, policies, standard, guidelines and how they work together to deliver identified security outcomes. Awareness of legal framework, key concepts applying to ISO27001 (a specification for information security management), and awareness of legal and regulatory obligations for breach notification.



Progression:

This apprenticeship is recognised for entry to both IISP and BCS Associate Membership and for entry onto the Register of IT Technicians confirming SFIA level 3 professional competence. Those completing the apprenticeship are eligible to apply for registration.

Next steps:

To configure an ideal apprenticeship we will meet with you, discuss your needs, present the options and collaborate to determine the best apprenticeships to meet your needs. We will provide ongoing support including:

- Recruitment of candidates
- Quality assured information advice and guidance
- Updates and information on legislation and funding
- Support and guidance for apprentice and employer throughout the apprenticeship
- Access to a comprehensive suite of resources and support material via OneFile
- Industry specialist qualified trainers and mentors