Apprenticeships

GP STRATEGIES®

Cyber Security Technologist Level 4 Apprenticeship

Flexible and Blended Training Solutions

96% Apprentice Satisfaction Rate

Progression to Associate Level Certifications

Cyber Security Technologist Apprenticeship

The main purpose of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations systems and people. They also work on areas such as security design & architecture, security testing, investigations & response. As part of the role they 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 an organisation's requirements.

Entry Requirements

This programme is for employees in cyber security roles, whether newly recruited or already employed. Newly recruited employees should ideally hold a Level 3 or equivalent IT qualification on entry.

Maths and English

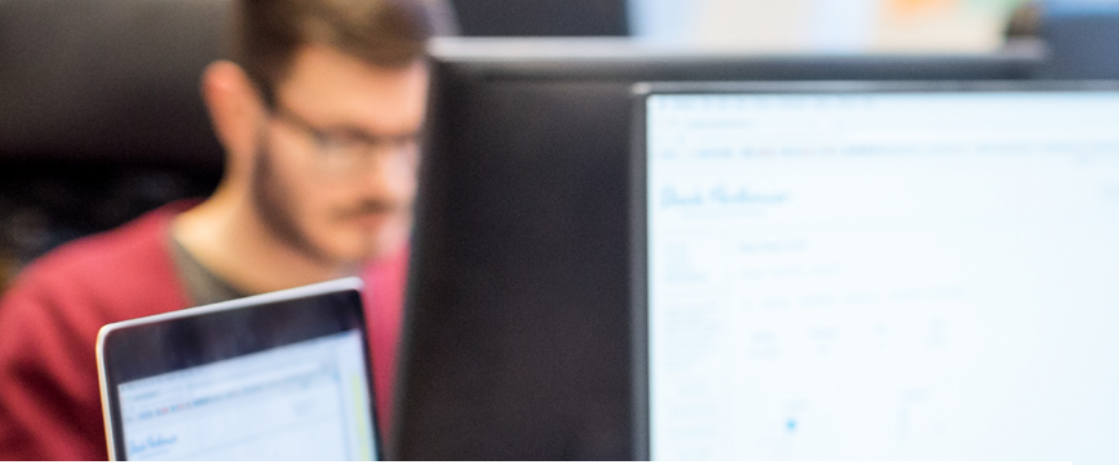
Apprentices achieve their Level 2 English and Maths qualification as part of their apprenticeship.

End Point Assessment (EPA)

Knowledge, skills and behaviours will be tested by an independent End Point Assessor, who will be appointed by your employer. Prior to your EPA, you will attend a Gateway Meeting with your employer, GP Strategies Skills Coach and your mentor/supervisor/manager, who will review your progress and confirm that all of the requirements of your apprenticeship have been met. You will then be referred for EPA.

The EPA will take the form of a summative portfolio, synoptic project, employer reference and interview and will be organised at a time and date convenient to both yourself and your employer. The vendor and module certifications, Self-Assessment and Level 2 Maths and English must be complete prior to the EPA taking place.

The outcome of your EPA test will be graded either Pass/Merit/Distinction/Fail.



Main Qualification Structure

Technical Competencies	
Threats, Hazards, Risks and Intelligence	Discover (through a mix of research and practical exploration) vulnerabilities in a system.
	Analyse and evaluate security threats and hazards to a system or service or processes. Be aware of and demonstrate use of relevant external sources of threat intelligence or advice (e.g. CERT UK). Combine different sources to create an enriched view.
	Research and investigate some common attack techniques and recommend how to defend against them. Be aware of and demonstrate use of relevant external sources of vulnerabilities (e.g. OWASP).
	Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.
Developing and Using a Security Case	Source and analyse a security case (e.g. a Common Criteria Protection Profile for a security component) and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern.
	Develop a simple security case without supervision. (A security case should describe the security objectives, threats, and for every identified attack technique identify mitigation or security controls that could include technical, implementation, policy or process).
Organisational Context	Identify and follow organisational policies and standards for information and cyber security.
	Operate according to service level agreements or employer defined performance targets.
Future Trends	Investigate different views of the future (using more than one external source) and trends in a relevant technology area and describe what this might mean for your business, with supporting reasoning.

Technical Competencies Continued	
Design build and test a network ("Build a network")	Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, that includes servers, hubs, switches, routers and user devices to a given design requirement without supervision. Provide evidence that the system meets the design requirement.
Analysing a security case ("Make the security case")	Analyse security requirements (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.), given for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.
Structured and reasoned implementation of security in a network ("Build a secure network")	Design and build a simple system in accordance with a simple security case. Provide evidence that the system has properly implemented the security controls required by the security case. The system could be either at the enterprise, network or application layer.
	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 given scenario/system.

Main Qualification Structure Continued...

Underpinning Skills, Attitudes and Behaviours
Logical and creative thinking skills
Analytical and problem solving skills
Ability to work independently and to take responsibility
Can use own initiative
A thorough and organised approach
Ability to work with a range of internal and external people
Ability to communicate effectively in a variety of situations
Maintain a productive, professional and secure working environment

Knowledge Modules

Module	Content	Certificated via
1. Cyber Security Introduction	• Why cyber security matters • Basic theory • Security assurance • How to build a security case • Cyber security concepts applied to ICT infrastructure • Attack techniques and sources of threat • Cyber defence • Relevant laws and ethics • The existing threat landscape • Threat trends	BCS Level 4 Certificate in Cyber Security Introduction
2. Network and Digital Communications Theory	Understands the basics of networks: • Data, protocols and how they relate to each other • The main routing protocols • The main factors affecting network performance including typical failure modes in protocols and approaches to error control	BCS Level 4 Certificate in Network and Digital Communications Theory

Knowledge Modules Continued...

Module	Content	Certificated via
3. Security Case Development and Design Good Practice	Understands, at a deeper level than from Knowledge Module 1, how to build a security case: • Describe what good practice in design is • Describe common security architectures • Be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance • Understands the importance of disaster recovery and how a disaster recovery plan works and their role within it	BCS Level 4 Certificate in Security Case Development and Design Good Practice
	Understand how to build a security case including context, threats, justifying the selected mitigations and security controls with reasoning and recognising the dynamic and adaptable nature of threats	
4. Security Technology Building Blocks	Understands how cyber security technology components are typically deployed in networks and systems to provide security functionality including: • Hardware and software	BCS Level 4 Certificate in Security Technology Building Blocks
5. Employment of Cryptography	Understands the basics of cryptography • Can describe the main techniques • The significance of key management • Appreciate the legal issues	BCS Level 4 Certificate in Employment of Cryptography

Duration

Typically this apprenticeship will take 18 – 24 months.

Typical Job Roles

The content is applicable to a variety of roles, including:

- Cyber Security Specialist
- Security Analyst
- Cyber Operations Manager
- Penetration Tester
- Information Security Officer
- Information

Progression

On completion, apprentices may choose to enter on to the Register of IT Technicians, to support their professional career development and progression.

Modules and vendor qualifications can also be a basis for continuing professional development in the apprentice's chosen field.

Qualification

Microsoft Technology Associate (MTA) qualifications are certified by Microsoft and are delivered by GP Strategies under our Silver partner status. Where chosen, CompTIA and Cisco certified qualifications are delivered by GP Strategies under our learning partner status.

Level

This is a Level 4 apprenticeship.

Find Out More

Visit our website for more information about our apprenticeship programmes: *www.gpstl-apprenticeships.co.uk*

Still Confused?

Contact our expert team today for more information on this apprenticeship:

T 0330 1000 610
E apprenticeshipsUK@gpstrategies.com

GP STRATEGIES®

Apprenticeships

Start learning with GP Strategies Apprenticeships and contact us today

0330 1000 610 | www.gpstl-apprenticeships.co.uk | apprenticeshipsUK@gpstrategies.com

GP Strategies – committed to equality and valuing diversity