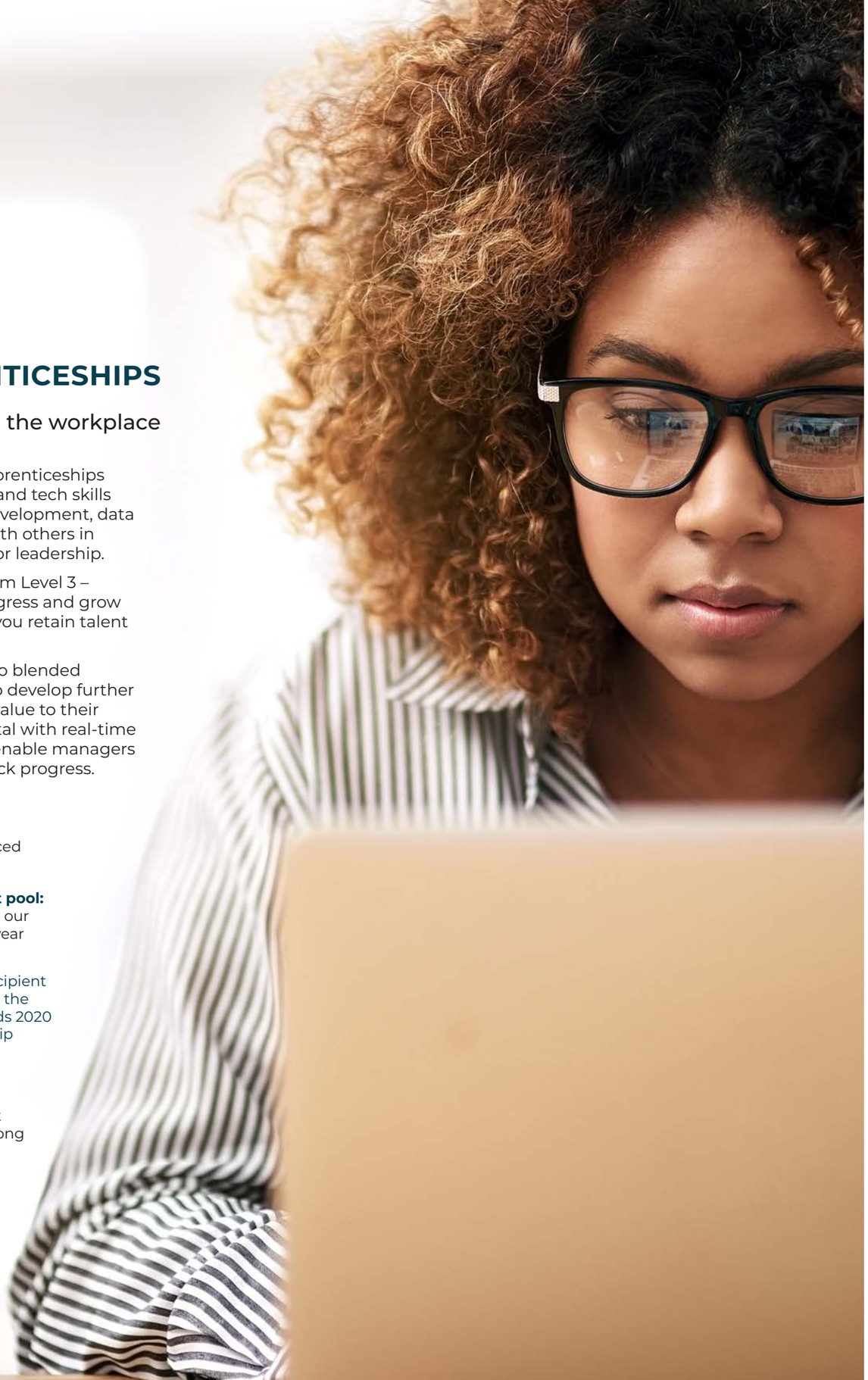
POWERING POTENTIAL

Apprenticeship Programme Guide

CYBER DEFENDER & RESPONDER

Level 4

QA.com



DIGITAL AND DEGREE APPRENTICESHIPS

Building tech careers in the workplace

We offer digital and degree apprenticeships that focus on the most in-demand tech skills including; cyber, IT, software development, data and digital marketing, along with others in project management and senior leadership.

With programme pathways from Level 3 – Level 7, we help learners to progress and grow within your company, helping you retain talent and build capabilities.

Our award-winning approach to blended learning enables apprentices to develop further and faster, adding immediate value to their roles, whilst our interactive portal with real-time dashboards and trigger alerts enable managers to effectively and efficiently track progress.

Experience: 30,000 apprenticeships placed

An unrivalled talent pool: 100,000 apply to join our programmes every year

Award-winning: Recipient of the Gold Award at the Learning Tech Awards 2020 for our apprenticeship delivery model

Proven: We have the highest overall pass rate among UK tech training providers*

*based on end-point assessments by the BCS 2020

CONTENTS

WHY QA?

We're the experts in Cyber apprenticeships

As the first to market for cyber security apprenticeships, we have been delivering Foundation Level programmes since 2012.

QA designed and delivered the first cyber security apprenticeship programme in the UK.

Our apprentices are initially working towards Level 4 with the opportunity to progress on to a Degree Apprenticeship after completion of their programme.

Our programmes are a blend of high-quality training, on-the-job experience provided by the employer, and the attainment of the Level 4 Cyber Security Technologist qualification.

Our Cyber Partner Community

QA partners with the leading experts in the Cyber Security industry. These relationships provide our customers with access to advanced technical training, cutting edge security research and industry expertise across a diverse range of topics.

Our partnerships are only with those who are at the top of their field and have a wealth of knowledge to share with like-minded individuals.

We offer additional skills with NCSP certifications

Our unique relationship with the NIST Cyber Security Professional (NCSP®) Programme, allows our cyber apprentices to have access to the NCSP® professional foundation certificate pathway and be eligible to take the exam, in addition to their apprenticeship.

OUR CYBER APPRENTICESHIPS HAVE EXCLUSIVE ACCESS TO PROJECT ARES®

Our Cyber apprenticeships have exclusive access to state-of-the-art gamified cyber skills learning platform, Project Ares®.

Our exclusive partnership with Circadence Corporation, the pioneer of the hands-on, gamified learning platform Project Ares®, allows us to uniquely incorporate hands-on scenario training into our cyber security apprenticeship, helping our cyber apprentices quickly build skills, knowledge and confidence in the cyber security disciplines needed to defend against hackers.

As the only UK training provider to use Project Ares in its cyber security training; the platform is a totally immersive experience, using automated features to support skills adoption with an in-game advisor 'Athena' who advises our players through the scenario-based challenges. With automated adversaries responding to players for added challenge.

This provides our apprentices with a scenario-based, gamified learning tool that drives high levels of engagement through leaderboards and badges, elements used widely in the gaming world.

The platform scenarios also replicate the unpredictability and escalating levels of complexity that cyber attacks can present, allowing the learner to develop problem-solving and critical thinking skills in a safe, but realistic environment.

Within this extended practice environment, we provide a safe place to apply all of the acquired skills throughout the programme, with added scoring of players and opponent actions with replay for objective assessment.

Ultimately actions culminate to inform models on best tactics for scenarios with instructor orchestration and observation.

The gamified learning Project Ares offers keeps the participant engaged and excited about continuous training, helping them see the true value of their capabilities.

Hands-on training and active-learning models increase retention rates by 75 percent, so our cyber apprentices can prepare for real-world challenges.

Other benefits of gamified learning include:

- Increased engagement, sense of control and self-efficacy
- Adoption of new initiatives
- Increased satisfaction with internal communication
- Development of personal and organisational capabilities and resources
- Increased personal satisfaction and employee retention
- Enhanced productivity, monitoring, and decision making

It works by enabling learners to apply what they know to simulated environments or "worlds," creating a natural flow that keeps learners engaged and focused in competitive, strategic situations.

SECURITY BLUE TEAM LEVEL 1

(complimentary)

The Security Blue Team level 1 certification is embedded within this apprenticeship programme.

BTL1 is designed primarily for individuals that are new to the industry, or are in junior positions that want to land a job or progress to a mid-level role.

Technical skills learned:

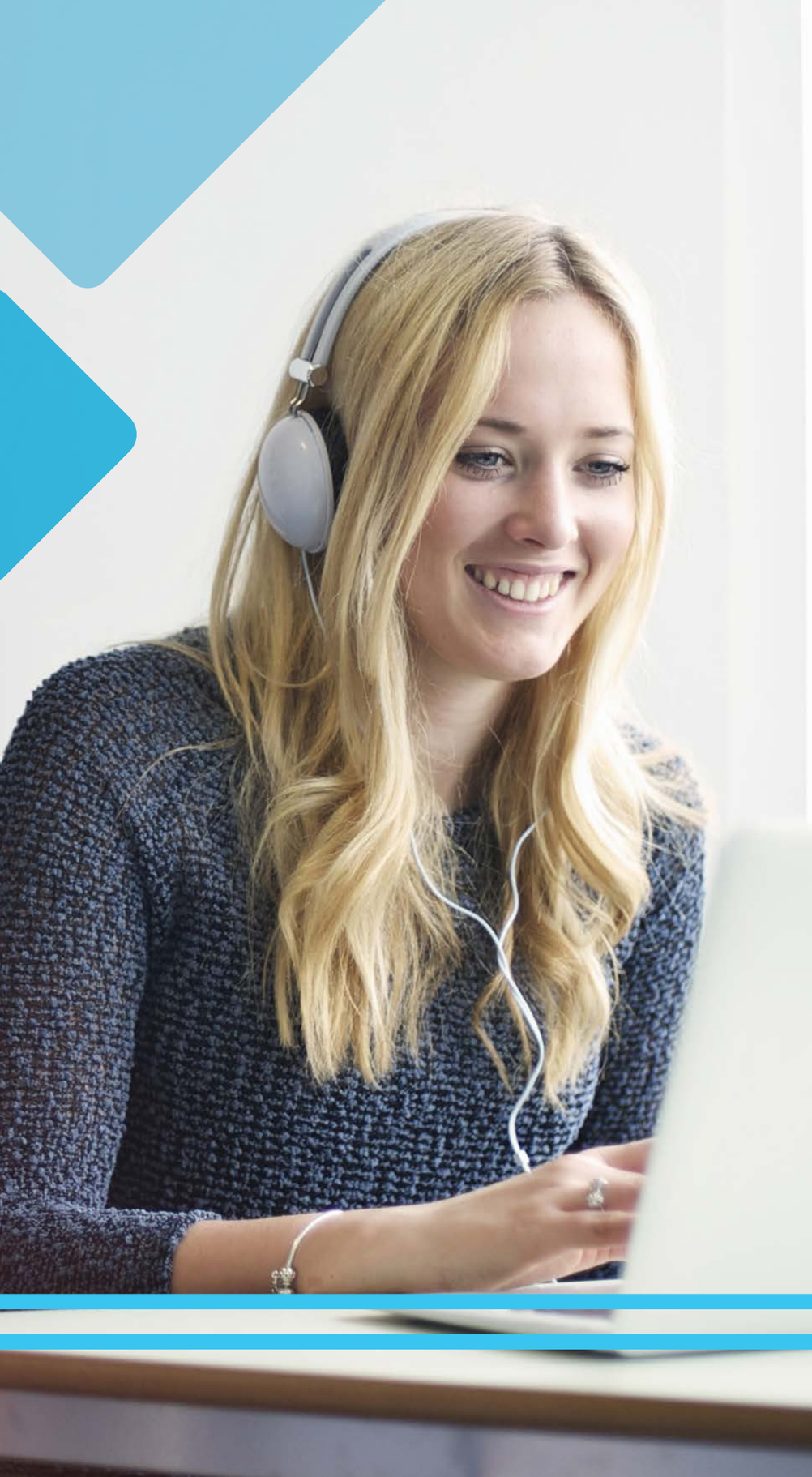
- Phishing Analysis
- Threat Intelligence
- Digital Forensics
- SIEM
- Incident Response

Students have the opportunity to take a practical 24-hour incident response exam certified by Security Blue Team within 12 months of the completion of Module 9.

Students will have access to a cloud lab via an in-browser demonstrating multiple ATT&CK Framework tactics.

- 70% = silver challenge coin
- 90% = gold challenge coin

One free resit voucher will be available in the event that learners do not pass their exam first time. This must be used within 12 months of completion of Module 9.



ROLE PROFILE

CYBER DEFENDER & RESPONDER

Cyber Defender & Responders apply an understanding of investigation techniques and analytical skills, to defend against and respond to cyber incidents within the network environment

Those in the Cyber Defender & Responder role will be typically more operationally focused, configuring and operating secure systems to prevent security breaches or monitoring systems to detect and respond to security breaches.

Cyber Defenders & Responders need:

- Strong analytical skills
- A methodical, step-by-step approach to resolving issues
- Business skills like effective communication, teamwork and task/time management
- The adaptability to do a range of work—sometimes complex and non-routine—in different environments
- The ability to work under direction, use discretion and determine when to escalate issues

JOB ROLE SUITABILITY

As an employer is it important to assess whether a candidate (a new hire or existing employee) is working in a suitable job role to successfully complete their programme.

The checklist has been created to help you assess whether your apprentice will be in a position to demonstrate all of the following Cyber Defender & Responders duties, during their programme.

Job roles this programme is a great match for:

- Cyber Security Analyst
- Threat Hunter
- Forensics & Incident Response Analyst
- Secure Operations Centre (SOC) Analyst, Network Intrusion Analyst,
- Incident Response Centre (IRC) Analyst,
- Network Operations Centre (NOC) Security Analyst

Checklist

1	Will they be identifying cyber vulnerabilities in a system to ensure security is maintained?
2	Will they be able to identify security threats and hazards to a system, service or process to inform risk assessments and design of security features?
3	Will they research and investigate into attack techniques and recommend ways to defend against them?
4	Will they be supporting cyber security risk assessments, cyber security audits and cyber security incident management?
5	Will they manage local response to non-major cyber security incidents?
6	Will they be configuring, deploying and using computer, digital network and cyber security technology?
7	Will they develop programme code or scripts for a computer or other digital technology?
8	Will they be writing reports, giving verbal reports and presentations in the context of their cyber security role?
9	Will they be part of managing cyber security operations processes, in accordance with organisational policies and standards and business requirements?
10	Will they participate in cyber war gaming and simulations, both technical & non-technical?
11	Are they going to keep up-to-date with industry trends and developments to enhance relevant skills and take responsibility for their own professional development?
12	Will they respond to a suspected security incident/breach/intrusion in accordance with organisation procedures any defined service level agreements or performance targets?

ENTRY REQUIREMENTS

The entry requirements for this programme are as follows:

- An A Level in ICT
- OR An International Baccalaureate at Level 3 in ICT
- OR A Level 3 apprenticeship in a similar subject
- OR A BTEC Extended Diploma in IT (180 credits)

Experience (if the learner can't meet the qualification requirements):

A minimum of 1-year work experience in a Technical support role e.g., Help Desk. Should also be working at Level 2 in Maths and English.

FINDING NEW TALENT

We offer an extensive attraction and recruitment service for employers who are looking to use apprenticeships to bring new talent into their organisation.

We use multiple channels and tactics to attract people who are interested in and are passionate about building a career in tech. Our recruitment model combines vigorous AI assessments with 1-2-1 interviews to ensure we select apprentices of the highest calibre.

We are committed to increasing diversity in tech and to help achieve this, we work closely with special interest groups including; Code First: Girls, Stemettes and Young Professionals to ensure apprentices from all backgrounds are given the same opportunities, and to support us to close the gender and diversity gap in tech.

Proactively engaged with over **4,000** sixth forms/colleges and universities, attending careers fairs to ensure we reach talent first

QA attracts **100,000 applicants** a year for its apprenticeship and tech academy roles and has nearly 200,000 in its candidate database

Significantly higher than average gender balance with **37%** of our apprenticeship starts being female, compared to an industry average of 19%

14.2% of our applicant pool indicated they have a BAME background - higher than the industry average of 13.3%

DIVERSITY AND INCLUSION

We're passionate about diversity in tech

It's our mission to help eradicate the gender gap, and make sure equal opportunities are given to applicants from all backgrounds. We do this through our long-standing partnerships, QA-driven initiatives and use of trending tools and software.

Diversity-first candidate attraction

We've invested in using augmented copy checking tools to ensure language is inclusive, open to all and free from bias.

We use inclusive imagery throughout our campaigns – producing visual content that promotes diversity and inclusion.

Diversity partnerships

We forge partnerships with like-minded organisations who share our vision on STEM gender equality including Code First: Girls, Stemettes and Young Professionals.

We make tech skills accessible to all

We run free tech workshops including '**Teach the Nation to Code**' and '**Teach the Nation to Cloud**' so anyone can explore technology career opportunities.

Promoting inclusivity

We nurture relationships with influencers, schools, colleges and universities via events and interactive sessions to ensure learners from all backgrounds are given the same opportunities.

Initial Assessment

Every candidate goes through an initial assessment where their current knowledge, skills and behaviours are measured and mapped against the apprenticeship standard.

This process is an assessment of the apprentice's eligibility for an apprenticeship programme, and ensures they are placed on the right programme at the right time, This contributes towards a successful completion and a good learner experience.

A BLENDED APPROACH TO LEARNING

How we deliver

QA apprenticeships are designed to immerse the apprentice in their job role while providing time for them to complete the required off-the job training to become occupationally competent and ready to undertake End-Point Assessment to complete their apprenticeship standard.

QA Apprenticeships also provide more flexibility for the employer, allowing apprentices to learn through a combination of project and lab work, live events, self-research, self-paced learning and peer-to-peer learning.

Full-time apprentices (those that work 30 hours per week or more) will be required to spend at least 20% of the apprentice's normal working hours over the planned duration of the apprenticeship practical period on off-the-job training. This means the minimum requirement for apprentices working 30 hours or more per week is an average of 6 hours of off-the-job training per week (i.e. 20% of 30 hours) over the planned duration.

Employer coaching, shadowing and mentoring remain off-the-job training, however, there will be more defined requirements to guarantee this is directly related to the apprenticeship and will be part of the training plan.

LEARNER SUPPORT

Safeguarding at QA

Safeguarding means ensuring the safety and wellbeing of our learners.

At QA, this means ensuring our polices and processes promote and protect learner wellbeing and that while you are on programme, and that while on programme, we teach learners about the types of risk facing modern day British citizens.

This includes cyber risks, mental and physical health information, risks of radicalisation or grooming and much more.

Prevent at QA

Prevent is part of the Government's counter-terrorism strategy.

At QA, this means we teach our staff and learners about the four British values: democracy, rule of law, individual liberty and respect and tolerance.

We also work with Prevent partners to identify people at risk of being or causing terror related harm.

Mental Health at QA

Emotional and mental wellbeing is an important component of successful learning.

Understanding how to protect mental health and promote emotional wellbeing is part of modern British citizenship.

Ways to access support if you are worried for yourself or someone else:

- Call us – anytime 07808 050273
- Email: safeguarding@qa.com
- Contact your Digital Learning Consultant (DLC), tutor or account manager
- Speak to any member of QA staff onsite

DIGITAL BY DESIGN APPRENTICESHIP PROGRAMMES

Digital by Design programmes

QA Digital by Design apprenticeships provide a greater focus on online learning together with using live interaction where it adds the most value for learners.

It means that there is a single learner journey which brings teaching, coaching, learning and assessment into a single, repeatable flow for every module. This ensures that from the beginning of the programme there is a clear focus on successful completion of the end-point assessment (EPA).

In Digital by Design, these three elements will work together:

- The content
- The service and support
- The technology

Discover, practise and apply

All QA apprenticeships use a guided discovery approach to learning, as opposed to traditional methods of delivery such as live events. This shifts the emphasis from content delivery to our learners and their context, resulting in the apprentice feeling empowered to take ownership of their learning experience through the “Discover, Practise, Apply” model.

DISCOVER

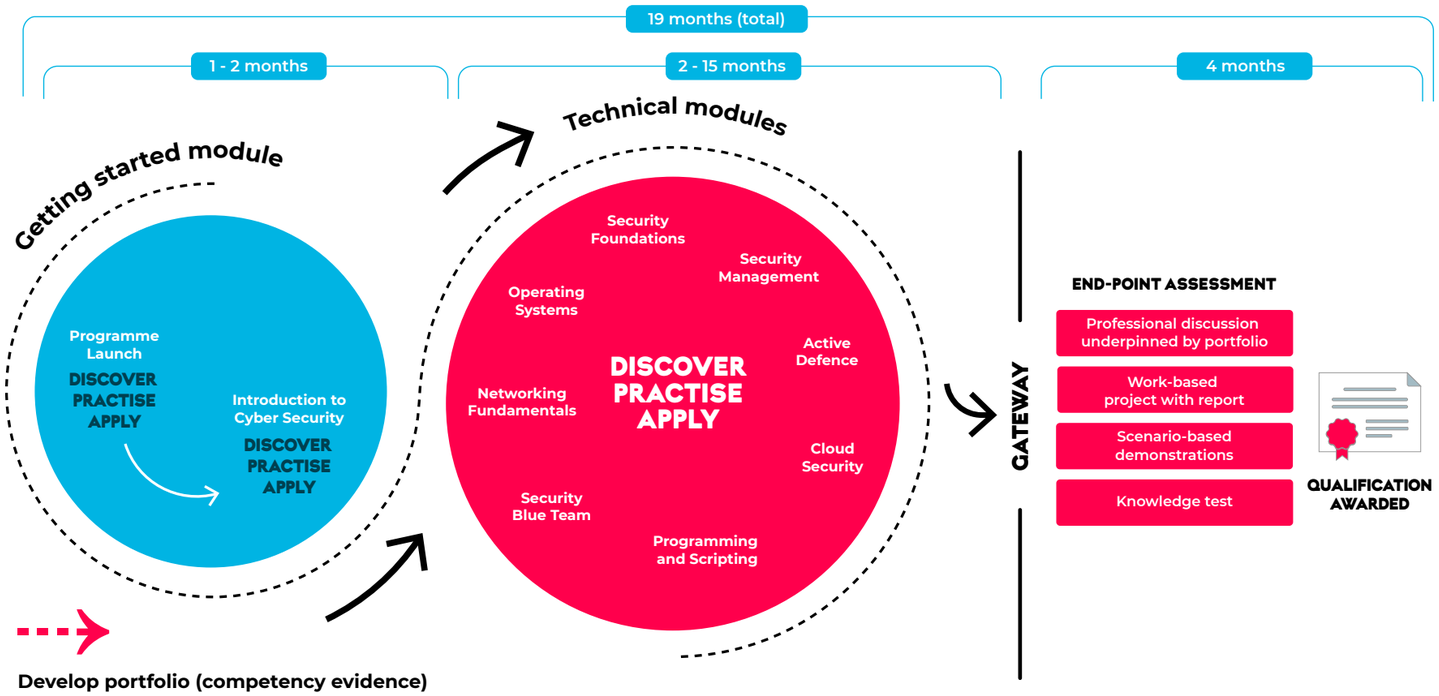
Learners will learn the theory, by exploring subjects online and in the live events.

PRACTISE

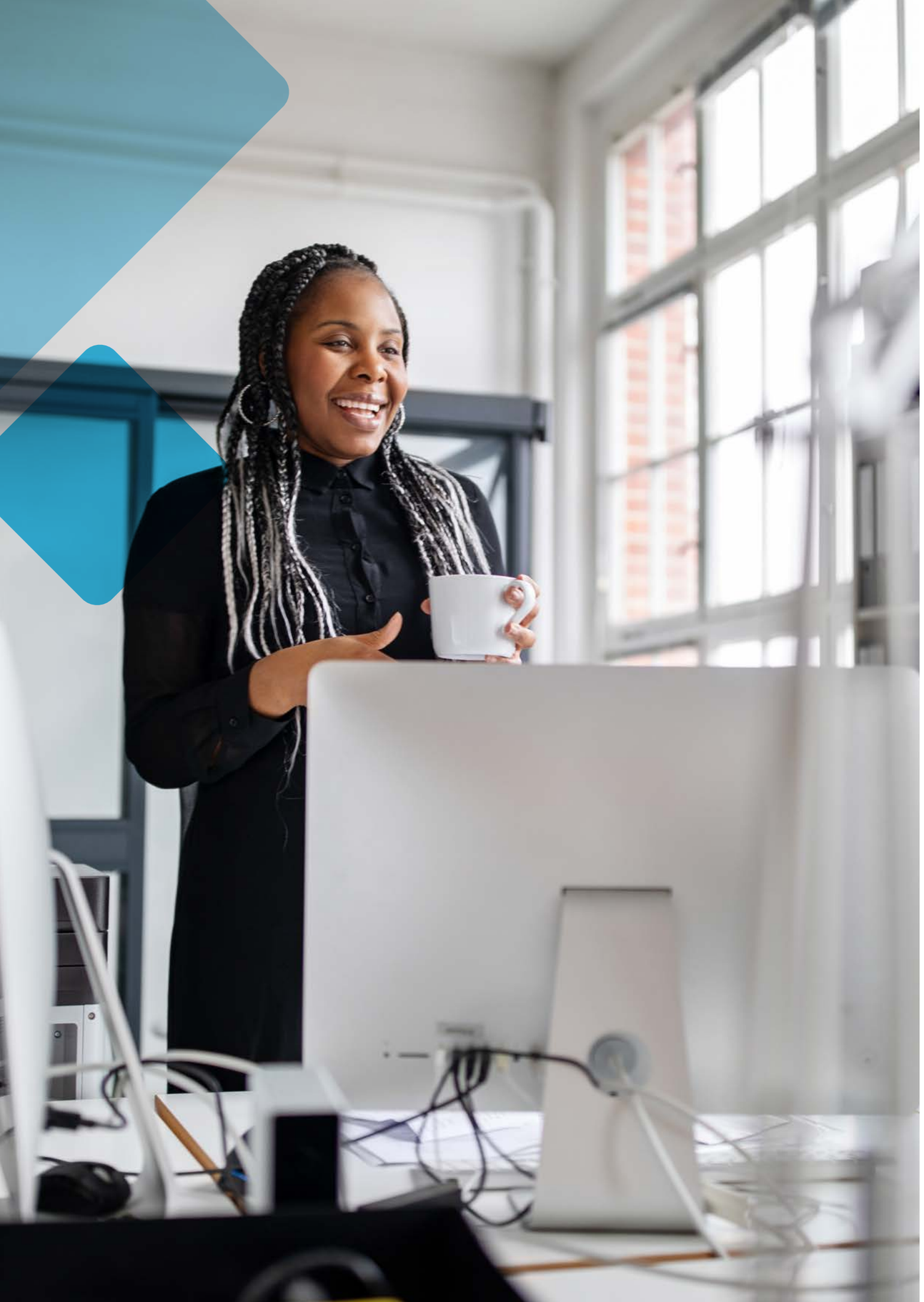
Learners will practise their new-found knowledge by completing activities - online, in the live events and (most importantly) directly at work in their day-to-day role.

APPLY

Learners will apply what they’ve discovered and practised at work. They will actively contribute to your organisation whilst building their portfolio of evidence (showing how they’ve applied their new skills) to gain their qualification.



Level 2 functional skills, English and Maths must be passed as part of the programme (if not already) and certificates presented, prior to taking the end-point assessment. This will be discussed at programme launch.



THE LEARNER'S JOURNEY

Programme timeline | Duration: 19 Months **| Gateway:** 15 Months

GETTING READY TO START

PROGRAMME LAUNCH

MONTH 1

- **Start Module 1:** Introduction to Cyber Security
- Safeguarding Module
- H&S: Workstation Assessment
- Functional Skills: Maths and English Diagnostics
- Functional Skills: Maths and English Learning
- **Check-in session**

MONTH 2

- **Employer Check-in**
- **End Module 1:** Introduction to Cyber Security
- **Start Module 2:** Networking Fundamentals

MONTH 3

- Functional Skills: Speaking, Listening and Communicating Exam Preparation
- Functional Skills: Maths and English (RandW) Mock Exams
- Functional Skills: Speaking, Listening and Communicating Exam
- Functional Skills: Maths Exam
- Functional Skills: English (R) Exam
- Functional Skills: English (W) Exam

MONTH 4

- **End Module 2:** Networking Fundamentals
- **Start Module 3:** Operating Systems

MONTH 5

- **End Module 3:** Operating Systems
- **Start Module 4:** Security Foundations

MONTH 7

- **End Module 4:** Security Foundations
- **Start Module 5:** Security Management
- **Employer Reflection (1 of 2)**

MONTH 8

- **End Module 5:** Security Management
- **Start Module 6:** Active Defence

MONTH 10

- **End Module 6:** Active Defence
- **Start Module 7:** Cloud Security

MONTH 11

- **End Module 7:** Cloud Security
- **Start Module 8:** Programming and Scripting

MONTH 12

- **End Module 8:** Programming and Scripting
- **Start Module 9:** Security Blue Team
- **Employer Reflection (2 of 2)**

MONTH 14

- **End Module 9:** Security Blue Team

MONTH 15

- **Portfolio Consolidated**
- **End-point Assessment Preparation**

Qualification Awarded

GETTING STARTED MODULE

The modules in our Cyber Defender & Responder apprenticeship equip learners with the advanced technical skills they need for their role. Each module develops the core set of skills they must be able to do well to be competent.

In each module, learners will 'discover', 'practice' and 'apply' what they've learned. This helps them put their newly-found knowledge into action back at work.

There are nine modules to complete with the following learning outcomes.

Module 1: Introduction to Cyber Security

Programme Launch
(Synchronous session online)

- Learn about the programme and structure
- Calendar of apprenticeship events
- Setting expectations
- Complete first Cyber activity – SWOT Analysis

Discover. Practise. Apply.

This module will introduce the learners to the world of Cyber Security & IT. It will focus on two areas; ITIL and a High-Level Introduction to Cyber Security – what Cyber Security is, its roles and importance in industry, and some common technologies within the industry.

It will cover the below areas:

- Service Management concepts
- Service Value Stream
- ITIL Practices
- Guiding Principles
- Computing and Network Fundamentals
- Cyber Security Fundamentals
- Governance and Risk
- Security Considerations

Module duration: 5 weeks

Classroom attendance: N/A

TECHNICAL MODULES

The technical modules focus on the knowledge and skills required of a Cyber Defender & Responder in detail. After each module learners will 'apply' what they've learned at work on current projects. Project Ares is blended into every module.

Module 2: Networking Fundamentals

This module will give the learners a hands-on discovery of networking covering both on premise and cloud networking infrastructures.

It will cover the below areas:

- Network computing
- Network communications
- Internet primer
- Networking security
- Modern communications
- Virtualisation and cloud tech
- Networking quiz
- Local Area Networks, topologies and the OSI Model
- IP addressing
- Internet working
- Applications and security management

Module duration: 7 weeks

Classroom attendance: 5 days

The classroom is based on the CompTIA Network+ material. The exam is not included as part of this apprenticeship.

Module 3: Operating Systems

This module will give the apprentice an opportunity to explore the Linux operating system. This will allow them to gain an understanding of administration, and why this knowledge is key in helping maintain a strong cyber security posture.

It will cover the below areas:

- Linux, Windows, Mac basics
- System architecture
- Package and software management
- Command Line Basics
- Partitions and file systems
- Scripting and databases
- System services
- Networking and security

Module duration: 6 weeks

Classroom attendance: N/A

Module 4: Security Foundations

This module will focus on building on the apprentice's Cyber Security-specific skills, to give them a strong base of security knowledge and common security tooling in the industry.

It will cover the below areas:

- UK law regulations
- Introduction to cryptography
- Security fundamentals
- Risk management
- Cryptography
- Network connectivity and security
- Secure network configuration
- Authentication
- Access control
- Securing hosts and data
- Securing specialized systems
- Application security
- Cloud security
- Organisational security
- Disaster planning and recovery

Module duration: 7 weeks

Classroom attendance: 5 days

Module 5: Security Management

This module will focus on how cyber security is viewed from a business angle, first discussing Agile Fundamentals and swiftly moving onto relevant security frameworks in the industry, such as ISO and NIST.

It will cover the below areas:

- Agile fundamentals
- What is a security framework?
- Introduction to ISO27001 & 2
- What is GDPR?
- NIST foundations
- Understanding cyber risks
- The NIST cyber security framework fundamentals
- Core functions, categories & subcategories
- Implementation tiers
- Developing framework profiles
- Cyber security improvement
- Cyber security controls factory mode
- Introduction to security cases
- How to develop a security case
- Risk and Impact

Module duration: 7 weeks

Classroom attendance: 3 days

Module 6: Active Defence

This module will focus on how businesses can be attacked and the steps that a threat actor may take to compromise a system. This will give the learner an insight to the potential attack vectors and help them identify potential vulnerabilities in a system.

It will cover the below areas:

- Attack and defence introduction
- OWASP top 10
- Penetration testing
- Encryption techniques and forensics
- Introduction to Burpsuite
- Reporting and presenting

Module duration: 6 weeks

Classroom attendance: N/A

Module 7: Cloud Security

This module covers cloud technologies and the various security concerns around this technology, such as monitoring and data protection.

It will cover the below areas:

- Cloud computing fundamentals
- Web fundamentals
- Intro to SIEM tools
- Cloud concepts and virtualisation
- Cloud security frameworks, principles, patterns and certifications
- Security technologies – AWS, Azure, GCP
- Assurance, data protection and compliance
- System monitoring and analysis
- SIEM usage

Module duration: 7 weeks

Classroom attendance: 5 days

Module 8: Programming and Scripting

This module will focus on the learner learning having hands-on learning of some common and useful programming & scripting languages.

It will cover the below areas:

- Python programming; data types and conditionals
- Python programming: strings, collections
- Regular expressions
- Functions
- PowerShell basics, keywords
- Pipelines in PowerShell
- PowerShell administration scripting and automation
- Linux scripting basics, keywords
- Pipelines in Linux
- Linux administration scripting and automation

Module duration: 5 weeks

Classroom attendance: N/A

Module 9: Security Blue Team

This module is designed to train technical defenders that are capable of defending networks and responding to cyber incidents.

It will cover the below areas:

- Security Fundamentals
- Phishing Analysis
- Threat Intelligence
- Digital Forensics
- SIEM
- Incident Response

For a full list **please visit here**

Module duration: 7 weeks

Classroom attendance: N/A

Gateway and end-point assessment Consolidation, preparation and assessment (Online)

This final component will get learners ready to go through the ‘gateway’.

The apprenticeship gateway is an internal QA process. It will ensure that your learner’s work is ready to be assessed by BCS. This exists to increase their chances of success.

At this pre-gateway stage, learners will:

- Consolidate and submit their portfolio
- Write a project proposal as required for their EPA

In addition to the items above, learners must have successfully completed all the Functional Skills exams (except exempt learners).

Once learners have met all the above criteria, they will go through the gateway. When approved, it takes up to 4 months from gateway to achievement.

During this time, learners will:

- Complete their simulation assessment and questioning
- Complete their interview

Qualifications earned

- Cyber Security Technologist Level 4 Apprenticeship
- Certified Blue Team Level 1

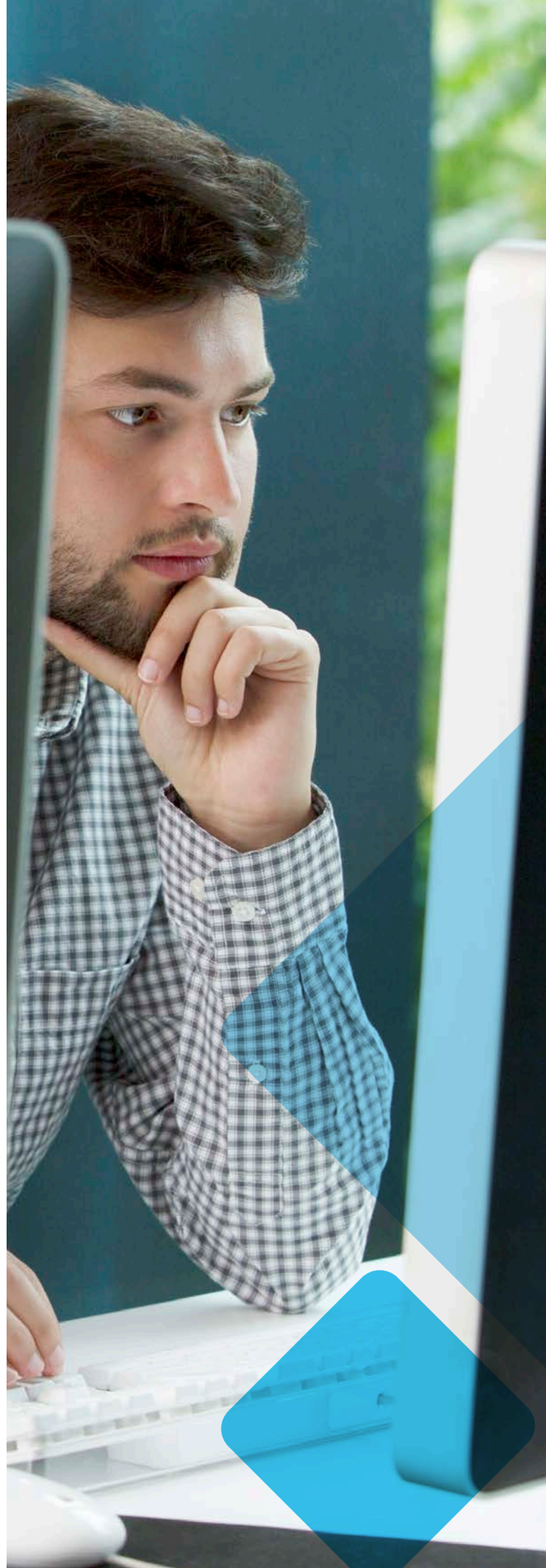
LEARNING OUTCOMES

Apprentices will be assessed on 3 key areas; their ability to convey knowledge, their ability to demonstrate practical skills and their capability of displaying professional workplace behaviour. These will be developed during an apprentice's learning journey, with the goal of displaying all of these competencies during their assessment.

These knowledge, skills and behaviour points ensure rounded development, as the standards provide a greater emphasis on the importance of both technical and soft skills in the workplace.

KNOWLEDGE

- K1: Principles of networks: OSI and TCP/IP models, 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; virtual networking
- K2: The concepts, main functions and features of at least three Operating Systems (OS) and their security functions and associated security features
- K3: Cyber security concepts and why cyber security matters to business and society; Security assurance concepts and how assurance may be achieved in practice including penetration testing and extrinsic assurance methods
- K4: The main types of common attack techniques; also the role of human behaviour, including the significance of the 'insider threat'. Including: how attack techniques combine with motive and opportunity to become a threat. Techniques and strategies to defend against attack techniques and mitigate hazards
- K5: The significance of identified trends in cyber security threats and understand the value and risk of this analysis. How to deal with emerging attack techniques (including 'zero day'), hazards and vulnerabilities relevant to the digital systems and business environment
- K6: Lifecycle and service management practices to an established standard to a foundation level for example Information Technology Infrastructure Library (ITIL) foundation level
- K7: Cyber incident response processes, incident management processes and evidence collection/ preservation requirements to support incident investigation
- K8: Understands the main features, applicability and how to apply the significant law, regulations and standards relevant specifically to cyber security. To include: laws, regulations & standards relating to personal data and privacy (e.g. Data Protection Act 2018 implementing General Data Protection Regulation); use of digital systems (e.g. Computer Misuse Act 1990); regulatory standards for cyber security, intelligence collection and law enforcement (e.g. Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000; standards for good practice in cyber security (e.g. ISO 27001, CyberEssentials, NIST) and any updates or additions
- K9: Ethical principles and codes of good practice of at least one significant cyber security professional body and the ethical responsibilities of a cyber security professional
- K10: How to analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification
- K11: Horizon scanning including use of recognised sources of threat intelligence and vulnerabilities
- K12: common security architectures and methodologies; be aware of reputable security architectures that incorporates hardware and software components, and sources of architecture patterns and guidance. How cyber security technology components are typically deployed in digital systems to provide security functionality including: hardware and software to implement security controls
- K13: The basic terminology and concepts of cryptography; common cryptography techniques in use; the importance of effective key management and the main techniques used; legal, regulatory and export issues specific to the use of cryptography
- K14: Risk assessment and audit methodologies and approaches to risk treatment; approaches to identifying the vulnerabilities in organisations and security management systems; the threat intelligence lifecycle; the role of the risk owner in contrast with other stakeholders
- K15: Principles of security management systems, including governance, organisational structure, roles, policies, standards, guidelines and how these all work together to deliver the identified security outcomes
- K16: Function and features of significant digital system components; typical architectures; common vulnerabilities in digital systems; principles and common practice in digital system security
- K17: Programming or scripting languages

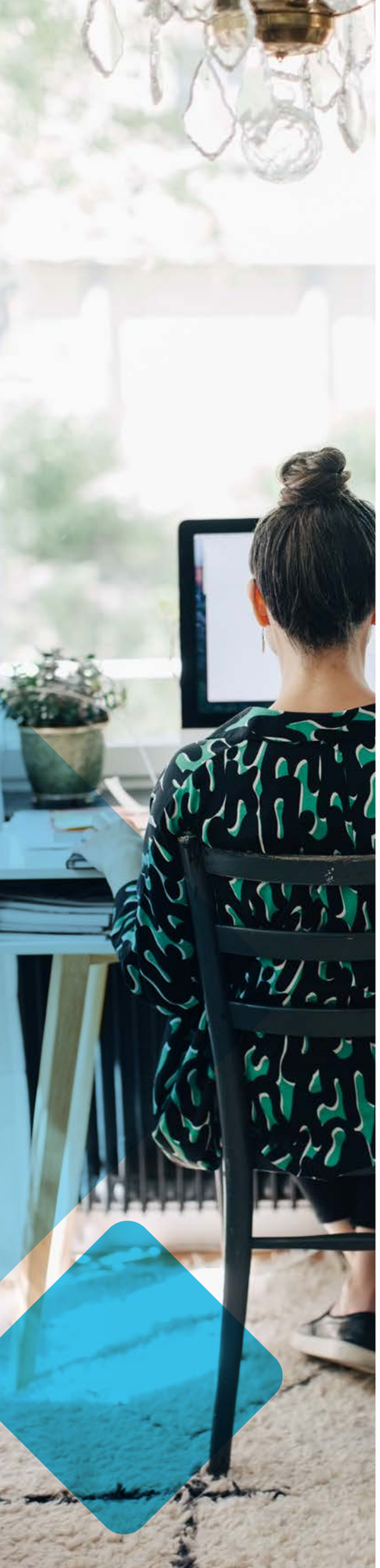


SKILLS

- S1: Discover vulnerabilities in a system by using a mix of research and practical exploration
- S2: Analyse and evaluate security threats and hazards to a system or service or processes. Use relevant external source of threat intelligence or advice (e.g. National Cyber Security Centre) Combine different sources to create an enriched view of cyber threats and hazards
- S3: Research and investigate common attack techniques and relate these to normal and observed digital system behaviour and recommend how to defend against them. Interpret and demonstrate use of external source of vulnerabilities (e.g. OWASP, intelligence sharing initiatives, open source)
- S4: Undertake security risk assessments for simple systems without direct supervision and propose basic remediation advice in the context of the employer
- S5: Source and analyse security cases and describe what threats, vulnerability or risks are mitigated and identify any residual areas of concern
- S6: Analyse employer or customer requirements to derive security objectives and taking account of the threats and overall context develop a security case which sets out the proposed security measures in the context with reasoned justification
- S7: Identify and follow organisational policies and standards for information and cyber security and operate according to service level agreements or other defined performance targets
- S8: Configure, deploy and use computer, digital network and cyber security technology
- S9: Recommend improvements to the cyber security posture of an employer or customer based on research into future potential cyber threats and considering threat trends
- S10: Design, build, test and troubleshoot a network incorporating more than one subnet with static and dynamic routes, to a given design requirement without supervision. Provide evidence that the system meets the design requirement.
- S11: Analyse security requirements given (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.) for a given system or product. Identify conflicting requirements and propose, with reasoning, resolution through appropriate trade-offs.
- S12: Design and build, systems in accordance with a security case within broad but generally well-defined parameters. This should include selection and configuration of typical security hardware and software components. Provide evidence that the system has properly implemented the security controls required by the security case
- S13: Write program code or scripts to meet a given design requirement in accordance with employers' coding standards
- S14: Design systems employing encryption to meet defined security objectives. Develop and implement a plan for managing the associated encryption keys for the given scenario or system.
- S15: Use tools, techniques and processes to actively prevent breaches to digital system security.
- S16: Conduct cyber-risk assessments against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.
- S17: Identify cyber security threats relevant to a defined context
- S18: Develop information security policies or processes to address a set of identified risks, for example from security audit recommendations.
- S19: Develop information security policies within a defined scope to take account of legislation and regulation relevant to cyber security.
- S20: Take an active part in a security audits against recognised cyber security standards, undertake gap analysis and make recommendations for remediation..
- S21: Develop plans for incident response for approval within defined governance arrangements for incident response.
- S22: Develop plans for local business continuity for approval within defined governance arrangements for business continuity.
- S23: Assess security culture using a recognised approach.
- S24: Design and implement a simple 'security awareness' campaign to address a specific aspect of a security culture.
- S25: Integrate and correlate information from various sources (including log files from different sources, digital system monitoring tools, Secure Information and Event Management (SIEM) tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a digital system security breach
- S26: Recognise anomalies in observed digital system data structures (including by inspection of network packet data structures) and digital system behaviours (including by inspection of protocol behaviours) and by inspection of log files and by investigation of alerts raised by automated tools including SIEM tools.
- S27: Accurately, objectively and concisely record and report the appropriate cyber security information, including in written reports within a structure or template provided
- S28: Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise
- S28: Configure digital system monitoring and analysis tools (e.g. SIEM tools), taking account of threat & vulnerability intelligence, indicators of compromise.
- S29: Undertake root cause analysis of events and make recommendations to reduce false positives and false negatives.
- S30: Manage local response to non-major incidents in accordance with a defined procedure.

BEHAVIOURS

- B1: Logical - Applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions
- B2: Analytical - working with data effectively to see patterns, trends and draw meaningful conclusions
- B3: Works independently and takes responsibility. For example works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges
- B4: Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit
- B5: Thorough & organised. For example uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time
- B6: Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion & diversity policy
- B7: Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences
- B8: Maintains a productive, professional and secure working environment
- B9: Creative - taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges
- B10: Problem Solving - Identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence



HOW TO GET READY FOR THE END-POINT ASSESSMENT

We want to deliver memorable learning experiences, whilst developing learners with well-rounded skillsets, ready to meet their professional requirements.

To ensure we are achieving this goal consistently, it is important for learners, digital learning consultants and employers to work together to ensure learners are supported to succeed in their apprenticeship's end-point assessment (EPA).

In this section we outline a number of guidelines which intend to provide a framework so that this can be achieved in a consistent way.

Preparation for the end-point assessment starts from day one.

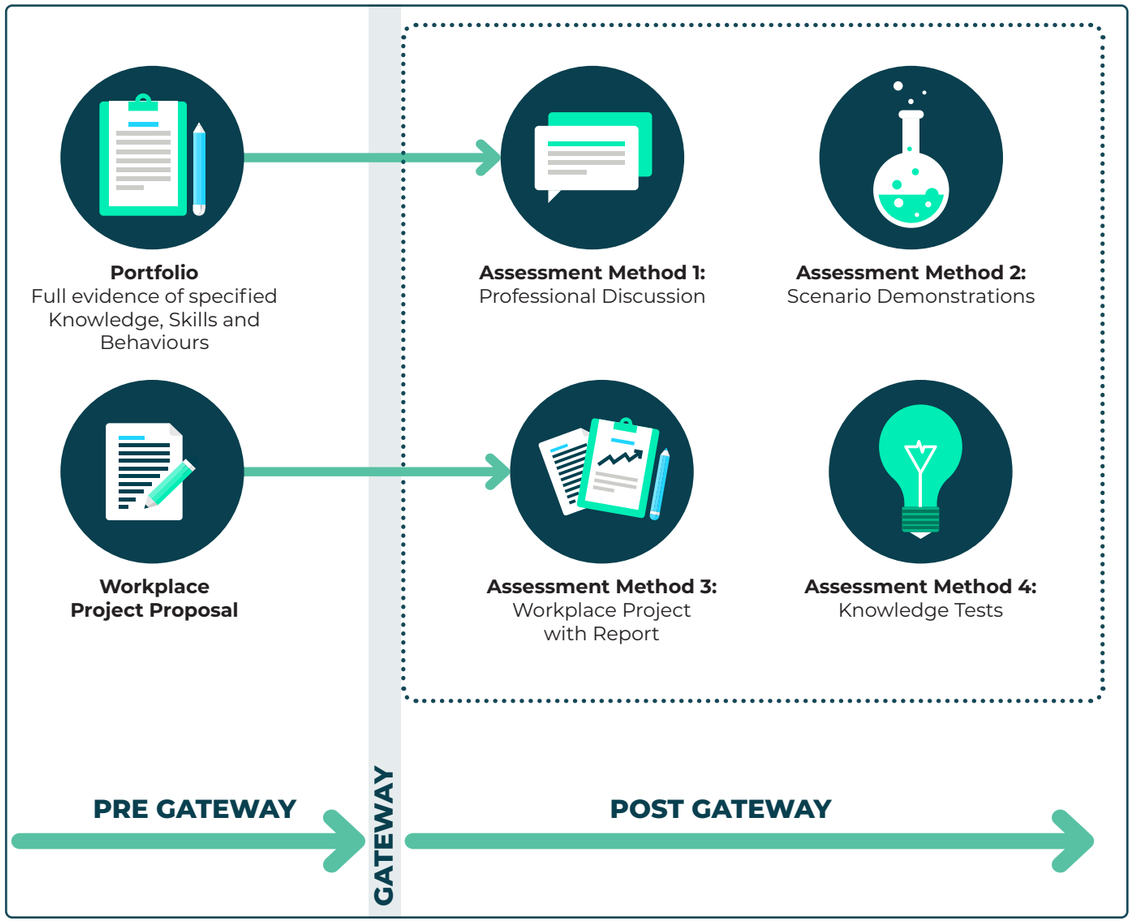
STAYING ON-TRACK THROUGHOUT THE PROGRAMME

Learners and employers should start preparing for EPA from the start of the programmme. Employers will need to ensure that learners are given the right opportunities at work to develop and prove the knowledge, skills and behaviours in the standard.

For this reason, it is very important to keep learners, digital learning consultants and employers informed about the programme progress. It is critical to the success of the apprenticeship programme that all of the above work together to ensure that each learning journey is kept on-track avoiding further interventions (and time commitment) whenever possible.

To help learners with this, we have created two guiding documents – a programme timeline, and a progress review map – so progress can be checked against it, at any time. Any progress deviations above 15% will be reviewed on a case-by-case basis. This is to ensure the apprenticeship is progressing in a timely manner.

HOW THE EPA IS GRADED



EXPANDING YOUR TECHNICAL SKILLS WITH cloud academy A QA COMPANY

Our apprentices are given full access to our proprietary Cloud Academy platform for the duration of their programme.

Cloud Academy brings the very latest and up-to-date content to our apprentices through single units, courses and comprehensive learning paths to really build on the core learning outcomes defined within the programme. Furthermore, apprentices are able to prepare for the full suite of vendor qualifications across AWS, GCP and Azure and much more.

Cloud Academy users also benefit from Hands-On Labs, Lab Challenges and Lab Playgrounds providing a safe, sandbox environment in which our learners are able to practise in real time through guided walkthroughs or through their own exploration.

Check out the Training Library - Cloud Academy.

FOR MORE INFORMATION, PLEASE CONTACT

0333 060 7701
qa.com/contact

V1.0 March 2023

This information is correct as of publishing in March 2023.

Funded by Department for Education

Funded by Education & Skills Funding Agency

European Union
European Social Fund

matrix

Apprenticeships

SKILLS FOR LIFE