



THE CYBER **SCHEME**

®

ADVANCING PROFESSIONAL STANDARDS
IN CYBER SECURITY

TRUSTED ASSURANCE FOR CYBER SECURITY CAPABILITY

THE CYBER SCHEME IS AN INDEPENDENT ASSURANCE BODY SPECIALISING IN TECHNICAL CYBER SECURITY ASSESSMENT, PROFESSIONAL REGISTRATION AND ACCREDITATION.

We make technical cyber security competence visible, measurable and recognised.

By combining assessment, professional registration, accreditation, training and workforce development, we help organisations strengthen capability, evidence professional standards and gain trusted assurance. Our work provides independent verification of competence, helping employers, clients, regulators and stakeholders make informed decisions based on demonstrated ability rather than self-declared expertise.

Our services support government bodies, critical national infrastructure, cyber security consultancies, training providers, employers and professional communities across the UK. Everything we do is centred on competence: demonstrated rather than assumed, assessed rather than claimed, and recognised against clear and consistent standards.

We believe that effective cyber security depends on capable people. That is why our activities focus on supporting the development, assessment and recognition of professional competence throughout a career. From those entering the profession through to experienced practitioners, managers and technical leaders, we provide structured pathways that help individuals develop capability, demonstrate achievement and gain professional recognition.

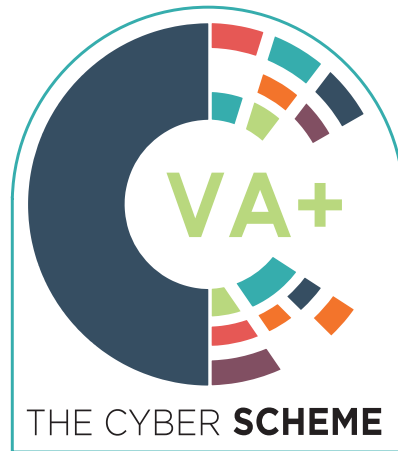
By connecting learning, assessment, accreditation and professional registration, we create an ecosystem that supports both individual career development and organisational capability. Together, these services help organisations build skilled workforces, raise standards, strengthen trust and demonstrate commitment to professional excellence.

Key benefits for organisations include:

- **Independent validation of technical competence**
- **Greater confidence in recruitment, retention and workforce development**
- **Support for government, regulatory and industry requirements**
- **Recognition and demonstration of professional standards**
- **Improved assurance for customers, partners and stakeholders**
- **Enhanced credibility, trust and market differentiation**
- **Clear pathways for skills development and career progression**
- **Stronger organisational capability through recognised professional practice.**



TRAINING, ASSESSMENT & CERTIFICATION



THE FOUNDATION OF TRUSTED CYBER CAPABILITY

Independent assessment sits at the heart of our approach. Our programmes provide objective evidence that individuals possess the knowledge, technical skills and professional judgement required to perform effectively in real-world cyber security roles, giving organisations a trusted benchmark for recruitment, workforce development, contractual requirements and government-aligned schemes.

Recognised throughout the UK cyber security community, our examinations are designed to assess practical competence rather than theoretical knowledge alone.

Candidates are required to demonstrate not only what they know, but how they apply that knowledge in realistic scenarios, reflecting the demands of professional practice.

Developed in collaboration with industry, employers and practitioners, our assessments remain relevant, rigorous and aligned with evolving workforce requirements.

Alongside assessment, we deliver training, mentoring and assessment preparation designed to build practical capability at every stage of a cyber security career. From those entering the profession to experienced practitioners, our programmes focus on developing the skills, behaviours and professional judgement required to operate effectively in the workplace.

By combining skills development with independent validation of competence, we help individuals build confidence, demonstrate capability and progress their careers, while providing employers with assurance that technical standards have been met through robust and objective assessment.

“CSTM is, in my view, superior to alternative certifications. Its combination of practical assessment, closed-book viva and reporting tests not just technical skills, but genuine understanding and the ability to justify decisions. The result is a rigorous assessment that reflects the realities of the role.”

Assessment candidate

PROFESSIONAL REGISTRATION

Licensed Body



For employers, registration supports recruitment, retention and workforce professionalisation while assuring clients, regulators and stakeholders that cyber security responsibilities are undertaken by appropriately qualified professionals. It also enables capable practitioners to gain recognition for their achievements and strengthens trust and accountability across the sector.

SUPPORTING PROFESSIONAL STANDARDS ACROSS THE CYBER SECURITY SECTOR

As the cyber security profession matures, employers and practitioners need recognised standards, clear career pathways and trusted indicators of professional competence.

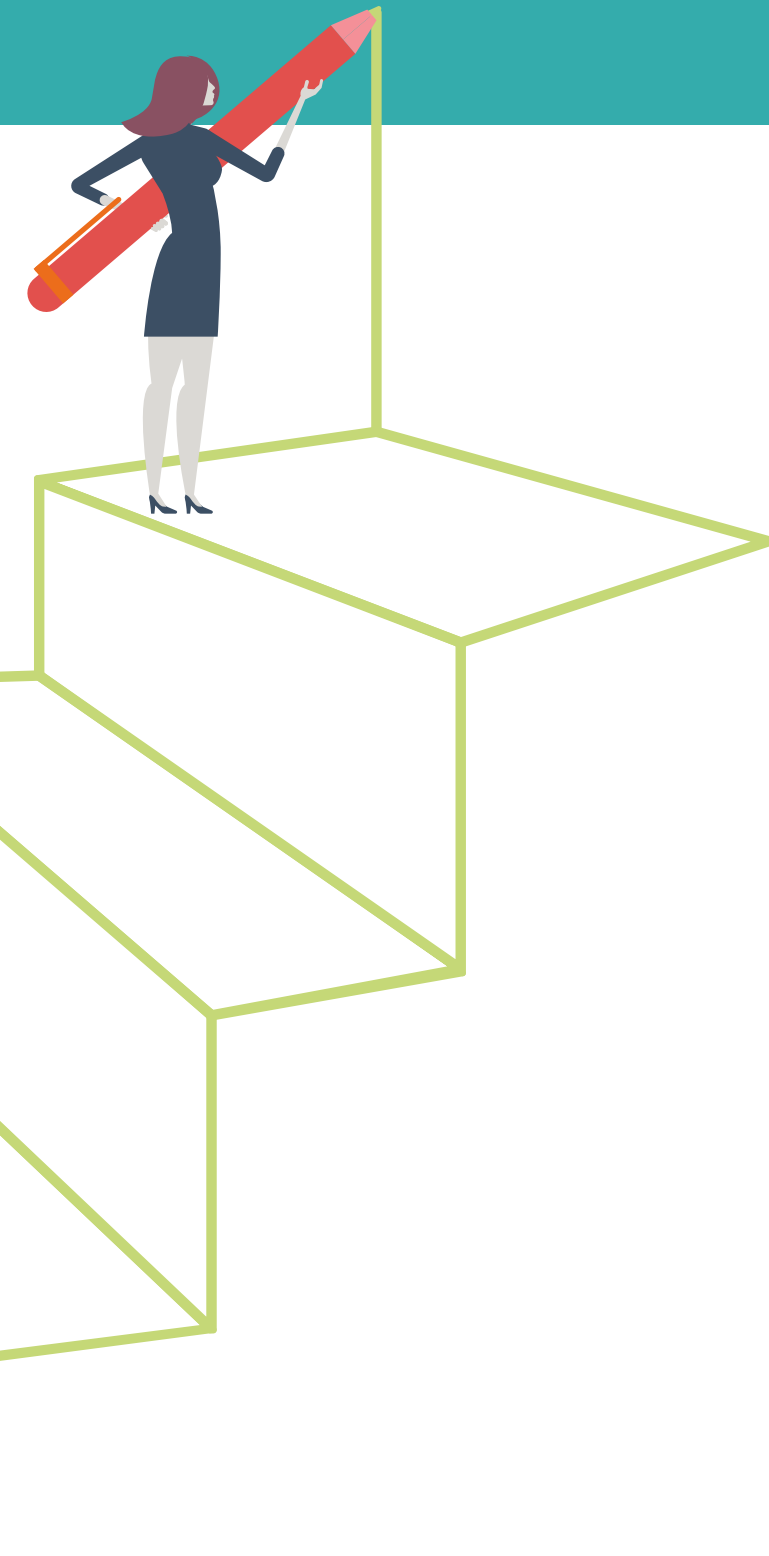
As a Licensed Body of the UK Cyber Security Council, The Cyber Scheme assesses and recommends individuals for Professional Registration across a range of specialisms and titles. Registration independently recognises competence, professional practice, real-world experience and commitment to continuing professional development against nationally recognised standards.

Key benefits for organisations include:

- Independent recognition of professional competence
- Alignment with nationally recognised standards
- Support for workforce professionalisation initiatives
- Improved confidence in capability and expertise
- Demonstrable commitment to professional development and ethical practice.

“ Professional cyber security titles demonstrate a unified standard of excellence to which you can align yourself. ”

UK Cyber Security Council



ACCREDITATION

BUILDING CONFIDENCE THROUGH RECOGNISED STANDARDS

Accreditation independently demonstrates that an organisation operates to recognised standards and is committed to quality, professional competence and continual improvement.

The Cyber Scheme offers routes for organisations delivering cyber security services and for providers of cyber security education and training. More than a badge or logo, accreditation gives customers, learners, partners and stakeholders structured assurance of capability, consistency and good practice.

Both accreditation pathways are designed to help organisations evidence capability in a clear, structured and recognised way. By providing independent assurance against defined standards, accreditation supports greater confidence in the quality, professionalism and credibility of the organisations delivering cyber security services and education.

For organisations, accreditation can help:

- Demonstrate commitment to quality and professional standards
- Build confidence with customers, learners and stakeholders
- Provide independent recognition of capability
- Support continual improvement and good practice
- Differentiate services in a competitive marketplace
- Strengthen reputation and credibility.

“Becoming accredited by The Cyber Scheme reflects our commitment to technical excellence, continual professional development, and providing our clients with confidence that they are working with independently recognised cyber security professionals.”

Sam Bramfitt, Bramfitt Technology Labs



ACCREDITED COMPANY PROGRAMME

Designed for organisations delivering cyber security services.

The Accredited Company Programme recognises organisations that place professional competence, workforce development and recognised standards at the heart of their services, giving customers and stakeholders greater confidence in their operations.

This programme is relevant for:

- Cyber security consultancies
- Security testing organisations
- Specialist technical service providers
- Organisations employing cyber security practitioners.



TRAINING CENTRE ACCREDITATION

Designed for organisations delivering cyber security education and training.

Training Centre Accreditation enables providers to demonstrate quality, consistency and alignment with recognised expectations, assuring learners, employers and purchasing organisations of high standards in cyber security learning.

This programme is relevant for:

- Commercial training providers
- Education organisations
- Specialist cyber academies
- Organisations delivering structured cyber security learning.

WORKFORCE DEVELOPMENT

DEVELOPING CYBER CAPABILITY ACROSS YOUR ORGANISATION

Strong cyber security depends on people who can apply knowledge in real-world environments, respond to changing risks and continue developing as the profession evolves.

The challenge is to understand existing capability, identify skills gaps and create practical pathways that support individual progression and organisational resilience.

Through skills gap analysis, technical development, assessment pathways, mentoring and professional progression routes, we help employers make informed workforce decisions and give practitioners the structure and support to progress with confidence.

“The need for Technical Investigators continues to grow and the complexity of existing and developing technology requires that the Investigators are trained and developed continuously. The Cyber Scheme continues to develop the Technical Investigators of the future.”

Roy Isbell, Editor, Digital Forensics Magazine.

Understanding Existing Capability

Through skills gap analysis and practical reporting, we identify strengths, development needs and areas requiring support. This creates a clear view of current capability and informs development strategies aligned to organisational objective-not generic training recommendations.

Flexible Development Pathways

We create pathways that reflect each organisation's priorities and workforce structure—from cohort-based programmes to flexible, modular approaches that accommodate operational responsibilities. Individuals can begin at different levels and progress towards technical, professional or assessment-related goals.

From Knowledge to Practical Confidence

Development is most valuable when learning can be applied in practice. We help individuals build the confidence, judgement and practical capability expected of competent professionals, aligning activity with recognised standards, technical assessments and progression routes so that learning leads to meaningful outcomes.

Supporting Long-Term Professional Growth

Capability is rarely built through a single intervention. By connecting assessment, development, mentoring, professional registration, accreditation and organisational assurance, we create structured pathways from learning to recognised outcomes and long-term professional growth.



PARTNERSHIPS & SECTOR ENGAGEMENT

WORKING ACROSS THE CYBER SECURITY ECOSYSTEM

Advancing cyber security capability and professional standards requires collaboration across government, professional institutions, employers, training providers and industry.

Through partnerships, advisory activity and sector engagement, The Cyber Scheme supports recognised standards, assessment pathways and assurance frameworks, ensuring our work remains practical, relevant and aligned to the profession's needs.

KEY PARTNERSHIPS



National Cyber
Security Centre
a part of GCHQ

The National Cyber Security Centre plays an important role in UK cyber capability. Our work with NCSC-aligned initiatives and assurance programmes helps organisations and professionals demonstrate competence against recognised standards while keeping assessments and development activity relevant to employers, practitioners and government-backed schemes.



Department for
Digital, Culture,
Media & Sport

The Cyber Scheme works with the Department for Culture, Media and Sport (DCMS) on cyber security capability and professional standards, contributing practical insight from technical assessment, professional registration and workforce development to inform UK skills, standards and capability.



The UK Cyber Security Council is the chartered professional body responsible for setting standards across the profession. As a Licensed Body, The Cyber Scheme assesses and recommends individuals for registration across multiple specialisms and title levels, supporting clear pathways and greater consistency in the recognition of competence.



IASME is a key partner in nationally recognised cyber security assurance schemes. Through initiatives including Cyber Advisor and Cyber Essentials-related activities, we help organisations access qualified professionals, trusted guidance and recognised standards.

ENGAGING WITH THE PROFESSION

We engage with employers, training providers, practitioners and industry stakeholders to understand workforce challenges and emerging disciplines. This keeps assessments current, standards relevant and development pathways aligned to professional need.

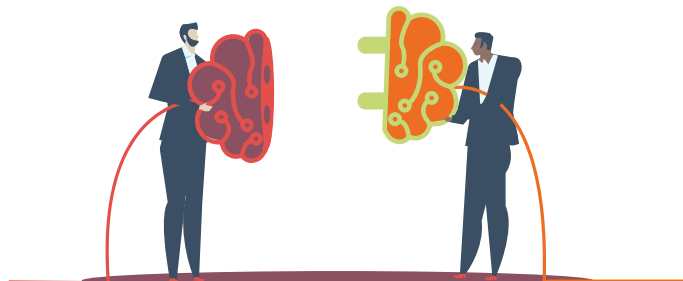
Contributing To Professional Standards

Working with industry and government, we contribute expertise on professional standards, technical competence and workforce capability. Through standards, frameworks and assurance activities, we help bring greater clarity to competence in practice.

Supporting Accredited Organisations And Training Providers

Accredited organisations and recognised training providers are central to our ecosystem. Accreditation demonstrates commitment to competence, standards and continual improvement, while training providers develop future practitioners and support growth.

By connecting learning, assessment, accreditation and recognition, we have created clear pathways for competence to be developed, demonstrated and recognised.





**WHETHER YOU NEED TO ASSESS CAPABILITY,
DEVELOP YOUR WORKFORCE, ACHIEVE
ACCREDITATION OR EMBED RECOGNISED
PROFESSIONAL STANDARDS, TALK TO
THE CYBER SCHEME ABOUT HOW WE CAN HELP.**



Training Course

Cyber Advisor Assessment Provider