



BECOMING AN ACCREDITED TRAINING CENTRE

BUILDING THE FUTURE OF CYBER SECURITY TRAINING TOGETHER

High quality cyber security training cannot be defined by content alone.

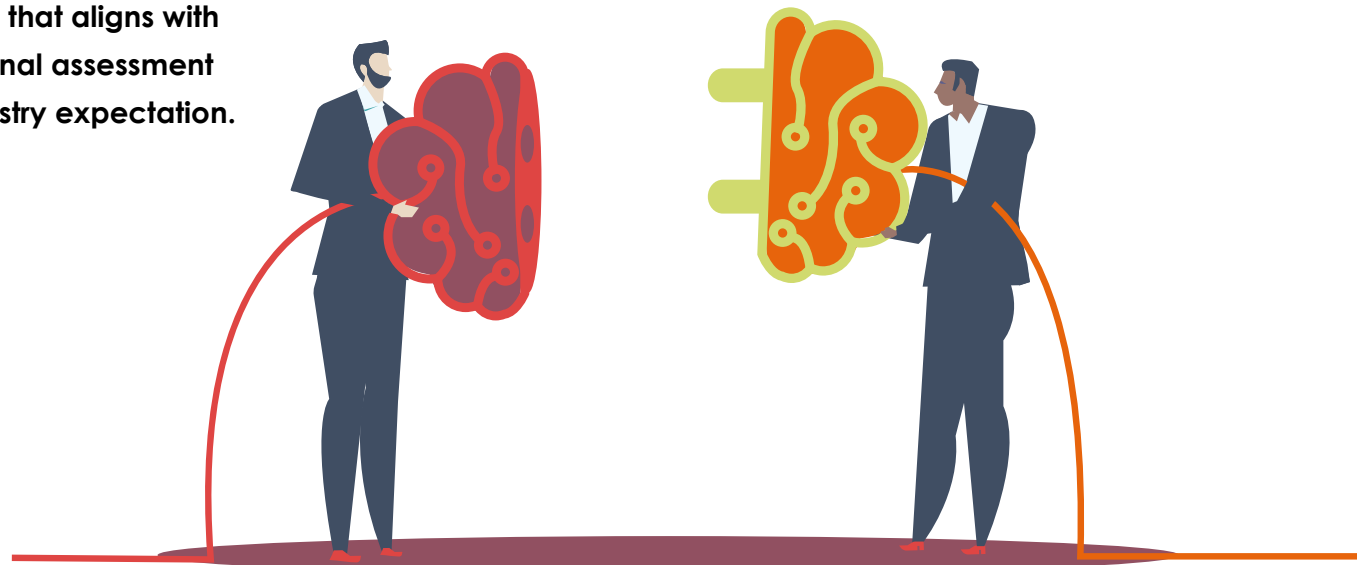
It is measured by its credibility, its relevance to real-world practice, and the confidence it gives to those relying on it.

This programme has been designed to recognise training organisations that can demonstrate not only technical depth, but also the ability to deliver structured, rigorous teaching that aligns with professional assessment and industry expectation.

At its core is a simple principle: training should not sit apart from assessment and professional standards, but be directly connected to them.

Our approach is to work with training providers who are already operating at a high level and support them in formalising that capability through a recognised framework, ensuring that what they deliver contributes meaningfully to the development of a capable, trusted cyber security workforce.

In doing so, we are not just accrediting training, but helping to shape how cyber skills are developed and sustained across the industry.



The Challenge

The cyber security training market is crowded and variable. Organisations and learners are increasingly seeking assurance that training aligns with recognised standards, reflects real-world practice, and supports professional development.

We will provide a framework through which high-quality training organisations can demonstrate that alignment.

Why become accredited with The Cyber Scheme?

The Cyber Scheme has established a strong position in the professionalisation of the cyber security workforce, working across industry, government and academia to define standards, develop assessments, and support structured career pathways.

As that work evolves, it is increasingly clear that training plays a critical role in determining whether those standards are meaningful in practice. Without alignment between training and assessment, there is a risk of inconsistency, fragmentation, and ultimately, reduced confidence.

The Accredited Training Centre programme addresses this directly, creating a clear and structured link between what is taught, what is assessed, and what is expected in the workplace.

Organisations that join the programme are not simply providers of training; they become part of a wider ecosystem that is actively shaping the future direction of cyber security capability, contributing to the development of courses, influencing standards, and ensuring that training remains relevant as the industry evolves.

For organisations already delivering high-quality technical training, accreditation represents an opportunity to lead within that space, strengthening both credibility and influence.



What Training Accreditation means

The intention of this programme is not to create an additional layer of process, but to provide a coherent structure through which training can be recognised, developed, and connected to professional outcomes.



By working in partnership with accredited training centres, we are able to ensure that courses are aligned to the competencies that underpin our assessments, and that candidates progressing through those courses are genuinely prepared for the demands of professional practice.

This creates clarity for employers, confidence for candidates, and a more consistent standard across the wider training landscape.

It also creates a collaborative environment in which training providers are able to contribute directly to the development of future pathways, helping to ensure that emerging specialisms, technologies, and methods are reflected in how training is designed and delivered.

What's in it for you?

Becoming an Accredited Training Centre places you within a recognised framework that signals both quality and intent, while also providing access to a more structured and engaged marketplace.

As part of the programme, your courses will be incorporated into The Cyber Scheme portfolio and promoted through official channels, giving them visibility to organisations and individuals actively seeking credible, assessment-aligned training.

At the same time, accreditation provides a clear marker of quality, demonstrating that your training is not only technically strong, but aligned to recognised standards and subject to ongoing quality assurance.

Beyond visibility, there is also the opportunity to play a more active role in shaping the future of cyber security training, contributing to the development of new courses, emerging specialisms, and evolving assessment requirements, ensuring that your organisation remains at the forefront of industry change.

For many organisations, this also creates a route to commercial growth, as demand increases for training that can be clearly linked to recognised standards and professional pathways.

Finally, accreditation provides a structured way to showcase your expertise, whether through your course portfolio, your instructors, or your contribution to thought leadership and industry development.

Key Benefits of Accreditation

- **Independent recognition**
- **Listing on The Cyber Scheme website**
- **Promotion through Cyber Scheme channels**
- **Alignment with recognised assessments**
- **Opportunity to influence future training pathways**
- **Enhanced employer confidence**
- **Demonstration of quality assurance**
- **Access to a network of leading providers.**

ATC Eligibility

To ensure consistency and credibility across the programme, organisations are required to demonstrate that they operate to recognised standards of both security and quality.

This includes independently audited certifications such as Cyber Essentials Plus for technical assurance, alongside broader organisational standards such as ISO 27001 or IASME Cyber Assurance.

Alongside organisational capability, there must also be clear evidence that the training itself is delivered by individuals with appropriate expertise and experience. For this reason, organisations are required to nominate at least one qualifying instructor for each course submitted for accreditation.

This combination of organisational assurance and individual capability ensures that accreditation reflects both the environment in which training is delivered and the quality of the delivery itself.

Who should apply?

Suitable for organisations that:

- Deliver technical cyber security training
- Offer instructor-led or blended learning
- Support professional certification pathways
- Want independent recognition of quality
- Maintain an active course portfolio.



Qualifying Instructors

Qualifying instructors are expected to demonstrate a depth of subject matter expertise aligned to the course content, supported by practical experience that reflects real-world application rather than purely theoretical knowledge.

Equally important is the ability to deliver training effectively, ensuring that complex material is communicated clearly and that candidates are supported in developing genuine understanding and capability.

Evidence of this may take a number of forms, including formal teaching qualifications, recognised instructional credentials, experience delivering training or presenting within the industry, or internal validation from organisations confirming observed delivery capability.

The intention is not to prescribe a single route, but to ensure that instructors can clearly demonstrate both competence and the ability to teach.

ATC Responsibilities

Accreditation carries with it a set of ongoing responsibilities, designed to maintain quality and ensure continued alignment with the wider objectives of the programme.

Training centres are required to operate transparently, allowing for periodic observation of course delivery, collecting feedback from candidates, and sharing anonymised data that helps inform continuous improvement across the portfolio.

There is also an expectation that training remains aligned to approved content, delivered by appropriately qualified instructors, and maintained at a level of activity that reflects genuine engagement with the programme.

Taken together, these requirements are not intended to be burdensome, but to ensure that accreditation remains meaningful, consistent, and trusted by those relying on it.

The Application Process

The application process has been designed to be structured but proportionate, focusing on demonstrating capability rather than navigating unnecessary complexity.

Organisations begin by preparing their application, ensuring that they meet the required organisational standards and have clearly defined training courses ready for submission.

From there, attention turns to instructors, with applications required to include evidence of expertise, experience, and delivery capability for at least one qualifying instructor per course.

**Prepare › Apply › Review ›
Approval › Onboarding ›
Ongoing Quality Assurance**

Once submitted, applications are reviewed in detail, with course content assessed for alignment to Cyber Scheme standards and the level of technical depth expected within the programme.

Where necessary, organisations may be asked to refine or strengthen elements of their submission to ensure consistency.

Course reviewers assess:

- Technical accuracy
- Learning objectives
- Practical relevance
- Course structure
- Instructor capability
- Alignment with Cyber Scheme standards.

Successful organisations will be approved as Accredited Training Centres and onboarded onto the programme, receiving guidance on delivery requirements, data sharing, and ongoing engagement.

Accreditation is maintained through continued participation, quality assurance, and alignment with programme expectations, ensuring that standards remain consistent over time.

Fees

The programme operates on a simple and transparent basis.

A one-off application fee of £1,200 is payable upon submission, followed by an annual fee of £1,200 to maintain accreditation.

All fees are exclusive of VAT.

Frequently Asked Questions

Do all instructors need to qualify?

No. At least one qualifying instructor is required for each course submitted.

Can existing courses be submitted?

Yes. Existing courses can be reviewed against programme requirements.

Is accreditation awarded to courses or organisations?

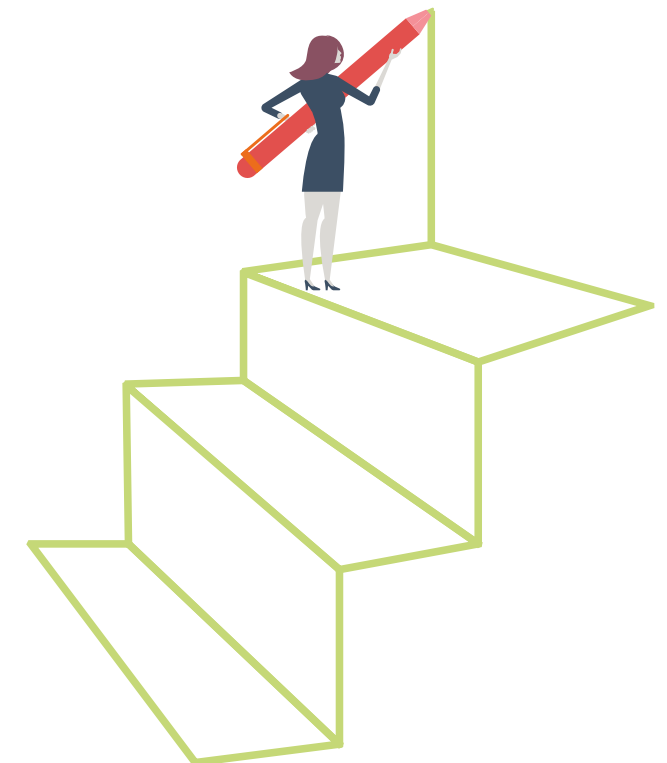
Organisations are accredited and individual courses are approved within the programme.

How long does accreditation last?

Accreditation is maintained through ongoing participation and annual renewal.

Successful organisations will receive:

- Accredited Training Centre status
- Use of the accreditation mark
- Website listing
- Promotional opportunities
- Access to programme updates
- Inclusion within future initiatives.





A clear route into recognised cyber training

The Accredited Training Centre programme establishes a direct and visible link between training, assessment, and professional recognition.

For organisations already delivering strong technical training, it provides a credible route to formal recognition, increased visibility, and closer alignment with industry expectations.

More importantly, it offers the opportunity to contribute to something broader: a more consistent, more trusted, and more capable cyber security workforce.

Help define the standards by which cyber security training is recognised.

If you are already delivering high-quality cyber security training and want to align it to recognised standards and professional outcomes, we invite you to apply.

Together, we can strengthen how cyber skills are developed, recognised, and trusted across the industry.



Training Course

Cyber Advisor Assessment Provider