THE CYBER SCHEME

CSFR

CYBER SCHEME FOUNDATIONS: RISK

CSFR

THE CYBER SCHEME

UNDERSTAND RISK. APPLY JUDGEMENT. BUILD PROFESSIONAL CONFIDENCE.

CYBER SECURITY RISK MANAGEMENT SITS AT THE HEART OF EFFECTIVE CYBER SECURITY.

Organisations need people who can understand what is at risk, assess the potential impact of threats, support informed decisions and communicate clearly with technical and non-technical stakeholders.

Cyber Scheme Foundations: Risk is a three-day practitioner course for people who want to develop a practical understanding of how cyber risk is identified, assessed, treated, governed, measured and communicated within organisations.

The course combines expert-led instruction with discussion, knowledge checks, individual activities, practical exercises and group-based scenarios. Participants apply the concepts throughout the course and bring them together in a final organisational case study.

WHY CYBER RISK MANAGEMENT MATTERS

Every organisation depends on information, systems, services and people to achieve its objectives. Understanding which assets matter, the threats they face and the consequences if those threats materialise is fundamental to making informed security decisions.

Cyber risk management provides a structured way to identify and assess uncertainty, decide where resources should be focused, select proportionate treatment and explain the available choices to those responsible for business outcomes. As cyber security becomes more closely connected with governance, resilience, compliance and organisational decision-making, these skills are relevant across a growing range of roles.

The course approaches cyber risk as an organisational discipline rather than an isolated technical or compliance activity. Participants examine how security concerns connect with business objectives, risk appetite, ownership, governance and professional judgement.

WHY THIS TRAINING IS DIFFERENT

The programme moves beyond definitions, checklists and risk-register administration. Participants consider how evidence is gathered, how assumptions influence an assessment, where uncertainty remains and how findings should be challenged and communicated.

Qualitative and quantitative approaches are explored alongside threat modelling, governance, compliance, recognised frameworks and meaningful measurement. Practical scenarios provide opportunities to apply the material in context and consider how different organisations may reach different but defensible decisions.

Independent accreditation by The Cyber Scheme provides assurance that the course structure, delivery approach and learning outcomes have been reviewed for quality and relevance to professional practice.

WHAT PARTICIPANTS WILL LEARN

BY THE END OF THE COURSE, PARTICIPANTS SHOULD BE ABLE TO:

- Explain the fundamental principles of cyber security risk and their relationship with organisational objectives.
- Identify and analyse assets, threats and vulnerabilities.
- Assess likelihood and impact using qualitative and quantitative approaches.
- Explain the difference between inherent and residual risk.
- Understand risk appetite, tolerance and capacity, and how these influence decisions.
- Identify appropriate treatment options, including acceptance, avoidance, reduction and transfer.
- Explain the difference between responsibility and accountability and understand who should own and manage a risk.
- Create and maintain meaningful risk information, including risk registers, treatment actions and residual risk.
- Use threat information and structured threat-modelling approaches, including data-flow diagrams and STRIDE.
- Understand how legislation, regulation, standards, policies and procedures influence cyber security risk.
- Explain the relationship between cyber risk, governance and compliance.
- Apply recognised approaches including ISO/IEC 27005, NIST and FAIR.
- Develop meaningful metrics to monitor risk and the effectiveness of controls.
- Explain how cyber risk influences systems architecture, incident management, disaster recovery and staff management.
- Communicate cyber risk clearly to technical and non-technical stakeholders.
- Apply risk management principles to a realistic organisational case study.
- Understand the professional registration framework and the responsibilities associated with registration.

WHO SHOULD ATTEND?

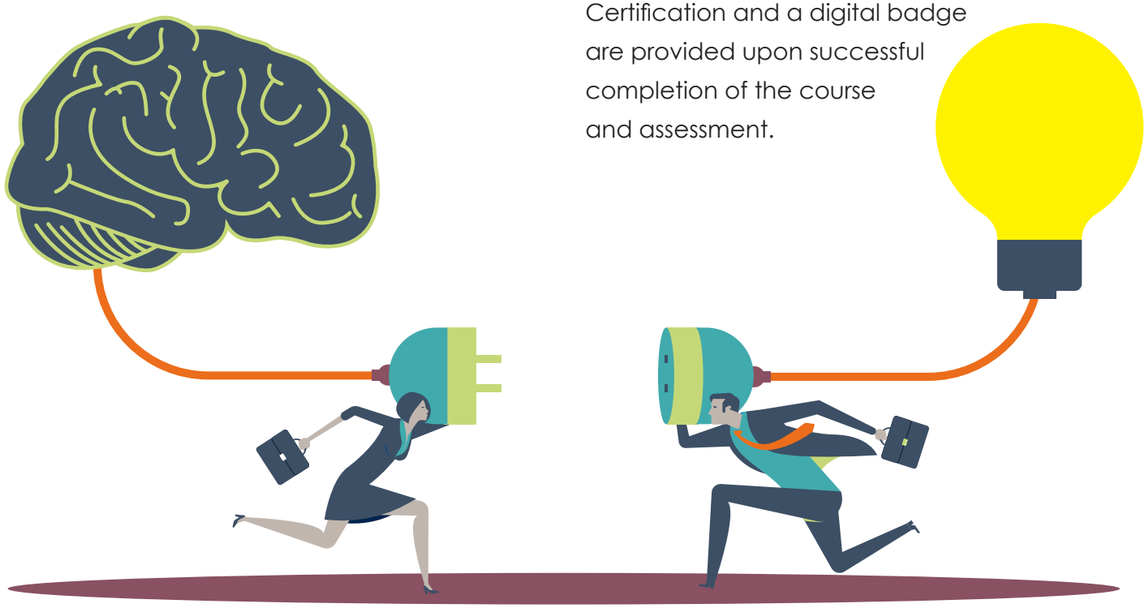
The course is intended for people entering or developing within cyber risk management and for professionals whose work requires a stronger understanding of how cyber risk should be assessed, governed and communicated.

- **Career changers and people at an early stage of a cyber career**
- **Junior cyber risk and GRC practitioners**
- **Cyber and IT professionals who contribute to risk decisions**
- **Audit and assurance professionals**
- **Governance, compliance and resilience teams**
- **Operational and project managers involved in risk activity**
- **Employers developing foundation-level cyber risk capability within their teams.**

PRACTICAL LEARNING AND ASSESSMENT

Learning is delivered through expert-led teaching, discussion, knowledge checks, individual activities, practical exercises and group-based scenarios. The emphasis is on applying risk concepts to realistic organisational situations rather than treating them as abstract models.

A final group case study asks participants to examine a business process, identify boundaries, threats and vulnerabilities, assess potential impacts and recommend proportionate treatment options.



EXAMINATION STRUCTURE

Participants complete a 90-minute examination comprising multiple-choice and short-form written questions on the afternoon of the final day. The assessment is designed to evaluate understanding of the course content and the ability to apply cyber risk management concepts in practice.

Additional time can be made available where an approved reasonable adjustment is required.

Certification and a digital badge are provided upon successful completion of the course and assessment.

THE CYBER SCHEME
ACCREDITED TRAINER

EXPERT-LED DELIVERY

Cyber Scheme accredited courses are delivered by experienced practitioners with recognised expertise in cyber security risk, governance, assurance and related disciplines.

All accredited instructors are assessed against The Cyber Scheme's requirements for technical competence, teaching ability and professional conduct. This ensures that every course is delivered by professionals with relevant industry experience and the ability to translate complex concepts into practical, real-world learning.

Courses combine established risk management principles, recognised frameworks and practical exercises designed to help participants apply their learning within their own organisations.

> "Effective risk management is not about producing a perfect answer. It is about understanding the evidence available, recognising uncertainty, applying professional judgement and communicating risk clearly to support better decisions."

Peter Loomes
Chartered Cyber Security Professional, Trainer and Instructor (Risk & Governance)

THE CYBER SCHEME

ACCREDITED BY THE CYBER SCHEME

The Cyber Scheme's Training Accreditation framework supports high-quality cyber security training that is relevant to professional practice and workforce development.

Accreditation provides independent review of course structure, delivery approach, learning outcomes and overall quality, giving learners and employers confidence that training has been assessed against recognised professional expectations.

Licensed Body

UK CYBER SECURITY COUNCIL

Assured Service Provider

in association with National Cyber Security Centre

Training Course

Delivery Partner

in association with National Cyber Security Centre

Cyber Advisor Assessment Provider