THE CSFR
(CYBER SCHEME FOUNDATIONS; RISK)

SYLLABUS

COURSE OVERVIEW

Cyber Scheme Foundations: Risk provides a practical introduction to the principles and practices of cyber security risk management. Participants move from the fundamental components of risk through assessment, treatment, ownership, governance, compliance, measurement and professional practice.

The course combines expert-led instruction with discussion, knowledge checks, individual activities, practical exercises and group-based scenarios. Participants apply their learning throughout the programme and complete a final organisational case study before the end-of-course examination.

Who the course is for

The course is intended for people entering or developing within cyber risk management, junior practitioners supporting risk or GRC activity, and cyber or IT professionals who need a structured understanding of risk, governance and compliance.

Entry requirements

- Participants should be able to take part in discussion, individual exercises and group activity.
- A supported Windows, macOS or Linux device capable of running a supported browser is required.
- Participants should preferably bring a laptop and charger, or a tablet.
- Pre-course preparation consists of reading the supplied course scenarios.

LEARNING OUTCOMES

On completion 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 inherent and residual risk.
- Understand risk appetite, tolerance and capacity.
- Identify appropriate treatment options.
- Explain responsibility, accountability and risk ownership.
- Create and maintain meaningful risk information.
- Use data-flow diagrams and STRIDE within structured threat modelling.
- Understand the influence of legislation, regulation, standards, policies and procedures.
- Explain the relationship between cyber risk, governance and compliance.
- Apply recognised approaches including ISO/IEC 27005, NIST and FAIR.
- Develop risk metrics and indicators.
- Explain how cyber risk influences architecture, incident management, disaster recovery and staff management.
- Communicate risk clearly to technical and non-technical stakeholders.
- Apply risk principles to an organisational case study.
- Understand professional registration and associated responsibilities.

COURSE SYLLABUS

1. Introduction to cyber risk

- What risk is and how it relates to organisational objectives
- Assets, threats, vulnerabilities, likelihood and impact
- Confidentiality, integrity and availability
- Risk appetite and organisational context
- Legislation and standards within risk management
- The risk management lifecycle.

2. Risk appetite, tolerance, capacity and ownership

- Risk appetite, risk tolerance and risk capacity
- Treatment options: accept, avoid, reduce and transfer
- Inherent and residual risk
- Risk ownership
- Responsibility and accountability
- The role of boards, management and operational teams.

3. Risk assessment methodologies

- Qualitative risk assessment and risk matrices
- Risk registers and residual risk
- Quantitative risk assessment
- Single Loss Expectancy, Annual Rate of Occurrence and Annualised Loss Expectancy
- Strengths, limitations and assumptions
- Introduction to probabilistic approaches.

4. Threat identification and threat modelling

- Common cyber threats
- Sources of threat information
- Data-flow diagrams and trust boundaries
- STRIDE threat modelling
- Prioritising threats using likelihood and impact
- Threat modelling during design and within existing environments.

5. Legislation, regulation, standards, policies and procedures

- How external obligations influence risk
- The distinction between legislation, regulation and standards
- Policies as organisational intent
- Procedures as operational execution
- Connecting mandatory requirements with proportionate risk management.

6. Governance, risk and compliance

- Organisational risk-governance structures
- Cyber risk as business risk
- Risk ownership and oversight
- The distinction between risk management and compliance
- Recognised approaches including ISO/IEC 27005, NIST and FAIR.

7. Metrics and control effectiveness

- The role of metrics in risk management
- SMART objectives
- Key Goal, Performance and Risk Indicators
- Annualised Loss Expectancy and Return on Security Investment
- Measuring control effectiveness
- Connecting measurement with governance and action.

8. The wider influence of cyber risk

- Systems architecture and defence in depth
- Incident management priorities and playbooks
- Disaster recovery, RTO and RPO
- Staff management, access, training and resources
- Professional registration, ethics and continuing development.

9. Integrated organisational case study

- Reviewing a business process
- Identifying boundaries, threats and vulnerabilities
- Assessing risk and impact
- Considering proportionate treatments
- Explaining and defending recommendations.

INDICATIVE SCHEDULE

Day one: Understanding cyber risk

Time	Session
09:30-09:35	Housekeeping
09:35-10:15	Introductions
10:15-11:15	What is risk and where is it?
11:15-11:30	Break
11:30-12:30	Risk appetite, legislation and standards
12:30-13:30	Lunch
13:30-14:10	Morning recap and risk-management lifecycle
14:10-15:00	Assets, vulnerabilities, likelihood and impact
15:00-15:15	Break
15:15-16:30	Risk tolerance, residual risk and ownership
16:30-16:45	Review of day one

Day two: Assessing and governing risk

Time	Session
09:30-09:50	Recap of day one
09:50-11:20	Qualitative and quantitative risk methodologies
11:20-11:35	Break
11:35-12:35	Common threats and threat identification
12:35-13:35	Lunch
13:35-13:50	Morning recap and questions
13:50-14:10	Standards, policies and procedures
14:10-14:55	Organisational structures supporting risk management
14:55-15:10	Break
15:10-15:40	Compliance principles
15:40-16:10	Common risk-management frameworks
16:10-16:25	Review of day two

Day three: Measuring and applying risk management

Time	Session
09:30-09:50	Recap of day two
09:50-10:50	Metrics and control effectiveness
10:50-11:05	Break
11:05-11:50	How risk influences other cyber security decisions
11:50-13:50	Integrated risk-management exercise
13:50-14:00	Professional registration
14:00-14:50	Lunch
14:50-16:20	End-of-course examination

Assessment

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

COURSE DELIVERY

- Expert-led instruction
- Discussion and question-and-answer activity
- Knowledge checks
- Individual activities
- Practical exercises
- Group-based scenarios
- Integrated case study

Training environment

- Standard training room with space for group work
- Internet access
- Projector and speakers
- Whiteboard and flipcharts
- Access to the examination environment

Delegate requirements

Device	Supported Windows, macOS or Linux device
Browser	A currently supported browser
Equipment	Preferably a laptop and charger, or tablet
Preparation	Read the supplied course scenarios
Accessibility	Reasonable adjustments can be made with prior notice

Contingency arrangements

- If the allocated room is unavailable, an alternative suitable room will be arranged. Online delivery may be considered only where appropriate and agreed.
- A local backup of course materials will be available if SharePoint or internet access is unavailable.
- If the interactive knowledge-check platform is unavailable, questions and activities will be delivered using a whiteboard or flipchart.
- If the examination platform cannot be accessed, the examination will be rescheduled or an approved alternative arrangement will be implemented.
- Equipment and examination access will be checked before delegates arrive.