

# Cyber Security Risk Assessment & Management

IT & IT Engineering  
Lisbon (Portugal)  
03 - 07 Feb 2025

UK Traininig

# PARTNER



## Cyber Security Risk Assessment & Management

**Ref:** 321388\_139373 **Date:** 03 - 07 Feb 2025 **Location:** Lisbon (Portugal) **Fees:** 4400 **Euro**

### Introduction

This Cyber Security Risk Assessment and Management course will teach you how to conduct a security risk assessment to protect your organisation. You will learn about the laws and regulations that impose strict cyber security requirements on all organisations, and gain the skills to develop a compliance assessment plan and employ a standards-based risk management process while maintaining a satisfactory security posture. Attendees should have a basic knowledge of business processes and technology concepts. No specialised technical knowledge is assumed

### Course Objectives:

- Implement standards-based, proven methodologies for assessing and managing the risks to your organization's information infrastructure
- Select and implement security controls that ensure compliance with applicable laws, regulations, policies, and directives
- Extend security protection to Industrial Control Systems ICS and the cloud

### Risk Assessment and Management Course Outline:

#### Day 1

##### Introduction to Risk Assessment and Management

- Ensuring compliance with applicable regulatory drivers
- Protecting the organisation from unacceptable losses
- Describing the Risk Management Framework RMF
- Applying NIST/ISO risk management processes

##### Characterising System Security Requirements

##### Defining the system

- Outlining the system security boundary
- Pinpointing system interconnections
- Incorporating the unique characteristics of Industrial Control Systems ICS and cloud-based systems

UK Training  
**PARTNER**

A decorative graphic in the bottom right corner shows a chessboard with several chess pieces, including a king, a queen, and a pawn, set against a background of concentric circles.

## Identifying security risk components

- Estimating the impact of compromises on confidentiality, integrity and availability
- Adopting the appropriate model for categorising system risk

## Setting the stage for successful risk management

- Documenting critical risk assessment and management decisions in the System Security Plan SSP
- Appointing qualified individuals to risk governance roles

## Day 2

### Selecting Appropriate Security Controls

### Assigning a security control baseline

- Investigating security control families
- Determining the baseline from system security risk

### Tailoring the baseline to fit the system

- Examining the structure of security controls, enhancements and parameters
- Binding control overlays to the selected baseline
- Gauging the need for enhanced assurance
- Distinguishing system-specific, compensating and non-applicable controls

## Day 3

### Reducing Risk Through Effective Control Implementation

### Specifying the implementation approach

- Maximising security effectiveness by "building in" security
- Reducing residual risk in legacy systems via "bolt-on" security elements

### Developing an assessment plan

- Prioritising depth of control assessment
- Optimising validation through sequencing and consolidation
- Verifying compliance through tests, interviews and examinations

### Formulating an authorisation recommendation

- Evaluating overall system security risk
- Mitigating residual risks
- Publishing the Plan of Action and Milestones POA&M, the risk assessment and recommendation

UK Training

**PARTNER**



## Day 4

### Authorising System Operation

#### Aligning authority and responsibility

- Quantifying organisational risk tolerance
- Elevating authorisation decisions in high-risk scenarios

#### Forming a risk-based decision

- Appraising system operational impact
- Weighing residual risk against operational utility
- Issuing Authority to Operate ATO

## Day 5

### Maintaining Continued Compliance

#### Justifying continuous reauthorisation

- Measuring impact of changes on system security posture
- Executing effective configuration management
- Performing periodic control reassessment

#### Preserving an acceptable security posture

- Delivering initial and routine follow-up security awareness training
- Collecting on-going security metrics
- Implementing vulnerability management, incident response and business continuity processes

UK Training

**PARTNER**



## Blackbird training cities

Accra1 (Ghana)

Amman (Jordan)

Amsterdam (Netherlands)

Annecy (France)

Baku (Azerbaijan)

Bali (Indonesia)

Bangkok (Thailand)

Bangkok (Thailand)

Barcelona (Spain)

Batumi (Georgia)

Beijing (China)

Beirut (Lebanon)

Berlin (Germany)

Birmingham (UK)

Bordeaux (France)

Boston,Massachusetts (USA)

Brussels (Belgium)

Cairo (Egypt)

Cape Town (South Africa)

Casablanca (Morocco)

Cascais (Portugal)

Copenhagen (Denmark)

Doha (Qatar)

Dubai (UAE)

Düsseldorf (Germany)

UK Traininig  
**PARTNER**



## Blackbird Training Category



Human Resources



Audit & Quality Assurance



Finance, Accounting, Budgeting



Marketing, Sales, Customer Service



Secretary & Admin



Law and Contract Management



Project Management



IT & IT Engineering



Supply Chain & Logistics



Management & Leadership



Professional Skills



Oil & Gas Engineering



Health & Safety



Telecom Engineering



Hospital Management



Customs & Safety



Aviation



C-Suite Training



Agile and Refinement



## Blackbird training Clients



UK Training  
**PARTNER**



**BLACKBIRD**  
FOR TRAINING

**LONDON TRAINING PROVIDER**



[www.blackbird-training.com](http://www.blackbird-training.com)



[training@blackbird-training.com](mailto:training@blackbird-training.com)



+44 7480 775526 / +44 7401 177335