BLACKBIRD FOR TRAINING

Cybersecurity Function Leadership and Cyber Risk Oversight Course

3 – 7 January 2027
Online



Cybersecurity Function Leadership and Cyber Risk Oversight Course

Ref: 105_363817 **Date:** 3 – 7 January 2027 **Location:** Online **Fees:** 2700 GBP

Introduction:

In this one-week Cybersecurity Function Leadership and Cyber Risk Oversight course, you learn to run your security function and oversee its cyber risk: set direction, structure policies and controls, fund the work, lead your people and report performance upwards. You build a cybersecurity function leadership plan that brings together a strategy statement, a governance charter, a risk register extract, a budget, a board dashboard and an improvement roadmap. You bring hands-on experience in security, IT or governance, risk and compliance work. You practise on a case study of a mid-sized organisation, judging its documents and data and defending your decisions.

Course Objectives:

- Draft a security strategy statement and governance charter for your own organisation using NIST CSF 2.0 Govern outcomes.
- Map your organisation's policies and controls against ISO/IEC 27001 and CIS Controls to expose gaps.
- Score your top cyber risks on a likelihood and impact matrix and set escalation thresholds for decision-makers.
- Build a security budget and team capacity chart that link every spending line to risk reduction.
- Present a one-page board dashboard of key risk and performance indicators for your security function.
- Test an incident escalation playbook and an awareness plan in a case study, then turn the lessons into an improvement roadmap.

Target Audience:

- You lead a security function or department and answer to senior management for its strategy and results.
- You run a security operations, engineering or architecture team and are taking on budget and people decisions.
- You work in governance, risk and compliance and write the policies, risk registers and reports that executives rely on.
- You manage IT services or infrastructure and carry security responsibilities alongside your operational role.
- You are a senior security analyst preparing to move into management and want to master the governance side of the job.



Course Outline:

Day 1: Setting the Security Strategy and Governance Model

- Assessing Current Security Posture Against NIST CSF 2.0 Profiles
- Aligning Security Strategy With Business Objectives Using Goal Maps
- Comparing Centralised, Federated and Hybrid Security Governance Models
- Assigning Security Roles and Accountabilities With a RACI Matrix
- Build: Security Strategy Statement and Governance Charter Draft

Day 2: Structuring Policies, Controls and Cyber Risk Decisions

- Structuring the Policy Hierarchy From Policy to Procedure
- Mapping Controls Across ISO/IEC 27001 and CIS Controls
- Rating Cyber Risks With a Likelihood and Impact Matrix
- Setting Risk Appetite and Escalation Thresholds for Decision-Makers
- Build: Policy Map and Cyber Risk Register Extract

Day 3: Allocating the Security Budget and Leading Security Teams

- Building a Security Budget With Run and Change Cost Lines
- Prioritising Security Spend Using Risk-Reduction Value Scoring
- Planning Team Capacity and Skills With a Competency Matrix
- Running Cross-Functional Collaboration With IT, Legal and Business Units
- Build: Security Budget Plan and Team Capacity Chart

Day 4: Analysing Security Performance and Leading Through Incidents

- Selecting Key Risk and Performance Indicators for Security
- Presenting a One-Page Board Security Dashboard With Trends
- Leading Incident Command Using Escalation Roles and Decision Logs
- Coordinating Crisis Communications Through an Executive Tabletop Exercise
- Build: Board Security Dashboard and Incident Escalation Playbook

Day 5: Applying Change and Improvement in a Security Case Study

- Designing a Role-Based Awareness Plan From Phishing Simulation Results
- Managing Resistance to Security Change With a Stakeholder Map
- Prioritising Strategic Security Initiatives on a Twelve-Month Roadmap
- Reviewing Maturity Gains Against the NIST CSF 2.0 Target Profile
- Build: Finalised Cybersecurity Function Leadership Plan



Skills You Will Gain:

- Security Posture Gap Analysis
- Governance Model Selection
- RACI Accountability Mapping
- Policy Hierarchy Structuring
- Cyber Risk Appetite Setting
- Risk-Reduction Value Scoring
- Competency Matrix Planning
- Tabletop Exercise Facilitation

Why Attend This Course:

- Leave with a cybersecurity function leadership plan built on your own organisation's context, ready to discuss with your manager.
- Practise defending risk and budget decisions in a case study, the way you will defend them in your next planning round.
- Rehearse your role in an incident tabletop exercise so that your first real escalation call feels familiar.
- Turn your security metrics into a one-page board view that you can reuse in your next management report.

Conclusion:

In your first week back, open your cybersecurity function leadership plan and replace the case study figures with your organisation's own risks, budget lines and team data. Then walk your manager, or the risk committee that oversees security, through the governance charter and the one-page dashboard, and agree the two initiatives to start first. After the first monthly report built from the plan, check whether the indicators moved, whether your team understood the escalation thresholds, and which policy gaps still need an owner.

Frequently Asked Questions FAQ:

What will you be able to do after the Cybersecurity Function Leadership and Cyber Risk Oversight course?

You will be able to set a security strategy, choose a governance model, oversee cyber risk, plan a security budget, lead a security team, report to executives and lead incident response, all tied together in one leadership plan for your organisation.



What do you need to know before starting a cybersecurity function leadership and cyber risk oversight course?

You need working experience in security operations, IT or governance, risk and compliance, and a basic grasp of risk and controls. Prior management experience is not needed: the course suits team leads and analysts moving into management as well as current security managers.

What do you build during the cybersecurity function leadership and cyber risk oversight course?

You build a cybersecurity function leadership plan, one piece a day: a strategy statement and governance charter, a policy map and risk register extract, a budget and team capacity chart, a board dashboard and incident playbook, then an awareness plan and improvement roadmap.

How does a cybersecurity function leadership and cyber risk oversight course differ from a general executive governance course?

This course stays inside the security function: its strategy, controls, cyber risk, budget, team, metrics and incidents. A general executive course covers boards, corporate strategy and finance across the whole organisation, while a technical security course trains you to operate tools rather than lead the function.

