
Board Cyber Risk Oversight Training Course: Appetite, Controls and Third Parties

30 November – 4 December 2026
Milan





Board Cyber Risk Oversight Training Course: Appetite, Controls and Third Parties

Ref: 319_21329 **Date:** 30 November – 4 December 2026 **Location:** Milan **Fees:** 5500 GBP

Programme Summary

Board cyber risk oversight is the subject of this five-day training course for directors, risk and compliance heads and business unit leaders, ending in a cyber risk oversight pack for one organisation or division. Cyber governance is often split between technical teams and committees that see only partial reports. The approach moves from roles and risk appetite, through risk assessment and controls, to third-party exposure and board reporting, then to a worked pack. Mars Training Centre UK delivers this programme in board cyber risk oversight.

The Business Case

Leaders who cannot say how much cyber risk the organisation accepts tend to learn the answer after an incident. Oversight that sets appetite, tests control assurance and tracks suppliers gives boards and executives evidence to challenge management and direct investment.

- Unowned Cyber Risks: Fall as appetite statements, owners and review cycles replace informal arrangements.
- Control Assurance Gaps: Narrow as leaders ask for evidence of control operation, not only policy existence.
- Third-Party Exposure: Reduces as supplier tiers, contract requirements and monitoring are set by risk.

Principles and Evidence Base

- NIST Cybersecurity Framework 2.0: Its Govern function, covering context, risk management strategy, roles and policy, structures the oversight work in Sessions 1 and 4.
- ISO/IEC 27005: Its guidance on information security risk management shapes the risk assessment and register work in Session 2.
- ISO 31000: Its principles and process for risk management guide the appetite, treatment and monitoring decisions in Sessions 1 and 3.

Intended Participants

- Directors who oversee enterprise risk and must challenge management on cyber exposure.
- Risk and compliance heads who maintain registers, policies and assurance plans.
- Business unit leaders who own processes, data and suppliers that carry cyber risk.
- Committee secretaries who prepare cyber reports for senior forums.

The programme serves banking, energy, healthcare and public-sector organisations.



Learning Outcomes

1. Participants will be able to define cyber governance roles and decision rights for a board, committee and executive team.
2. Participants will be able to construct a risk appetite statement with measurable cyber risk tolerances.
3. Participants will be able to evaluate a cyber risk register for ownership, rating logic and treatment status.
4. Participants will be able to diagnose assurance gaps by comparing control evidence with stated policy.
5. Participants will be able to prioritise supplier and third-party risks by tier and contract requirement.
6. Participants will be able to justify a board reporting pack and escalation rules to a committee chair.

Programme Structure

Day 1: Board Cyber Risk Oversight: Roles and Appetite

Who decides on cyber risk, and how much is the organisation willing to accept?

- NIST Cybersecurity Framework 2.0 Govern Function
- Decision Rights and Committee Mandate Map
- ISO 31000 Risk Appetite Statement
- Cyber Risk Tolerance Metrics
- Case Review of Two Sector Governance Failures

Day 2: Risk Assessment and the Register

How is cyber risk identified, rated and recorded in a way leaders can challenge?

- ISO/IEC 27005 Risk Assessment Process
- Cyber Risk Register Review
- Scenario Impact and Likelihood Rating
- Risk Owner Accountability Matrix
- Policy Framework Gap Review

Day 3: Controls, Assurance and Third Parties

What evidence shows that controls operate and suppliers are managed?

- Control Assurance Evidence Request
- Three Lines Assurance Map
- Supplier Tiering Model
- Contract Security Requirement Checklist
- Remediation Tracking Rules



Day 4: Reporting, Incidents and Escalation

What should a board see, and when must an issue be escalated?

- Board Cyber Reporting Pack
- Key Risk Indicator Set
- Incident Escalation Thresholds
- Regulatory and Customer Notification Roles
- Committee Challenge Question Set

Day 5: Applying Board Cyber Risk Oversight to One Organisation

Is the oversight pack ready for the committee chair and the executive sponsor?

- Applying the Session 1 Appetite Statement to the Chosen Organisation
- Testing the Session 2 Register Against Sample Scenarios
- Checking Session 3 Assurance Requests Against Supplier Tiers
- Applying the Session 4 Escalation Thresholds to Open Issues
- Completing the Cyber Risk Oversight Pack

Methodology

The programme is built around structured exercises and case analysis. Participants work with an anonymised organisation, a sample register and sample supplier and control evidence, set appetite, rate scenarios and draft reports in small teams, then defend their pack before a simulated board committee. No technical security background is required.

- Suggested activity: Writing three risk tolerances for a payments business.
- Suggested activity: Challenging a sample register entry that lacks an owner and a treatment date.
- Suggested activity: Tiering ten sample suppliers and choosing evidence requests for each tier.

Capstone Output

Each participant completes a cyber risk oversight pack for one organisation or division. It contains a decision rights map, a risk appetite statement, a reviewed risk register, an assurance and supplier plan, a reporting pack and escalation rules. It is used to brief the committee chair and executive sponsor.

Frequently Asked Questions

Is board cyber risk oversight suitable for directors without a technical background?

Yes. Board cyber risk oversight is set at managerial level and assumes responsibility for risk, compliance or business decisions, not technical security or programming skills.



Which frameworks does board cyber risk oversight rest on?

Board cyber risk oversight rests on the NIST Cybersecurity Framework 2.0 for governance, ISO/IEC 27005 for risk assessment and ISO 31000 for risk management.

How is the pack from board cyber risk oversight used at work?

You use the pack from board cyber risk oversight to brief your committee chair and executive sponsor, challenge management on evidence and set review cycles.

How does board cyber risk oversight differ from cyber security audit training?

Board cyber risk oversight centres on decisions, appetite and reporting by leaders, while cyber security audit training centres on testing controls and writing audit findings.