JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Information Security Leadership for CISOs Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Information Security Leadership for CISOs Training Course

Information Security Leadership for CISOs is a 1-week training course for chief information security officers, deputy CISOs and heads of security who must run security as a business function, and it produces a security leadership roadmap ready for executive endorsement. Boards now treat cyber exposure as an enterprise risk, so the security leader's influence depends on strategy, funding and credibility as much as on controls. Jupiter Prime Training delivers this information security leadership course.

Why Information Security Leadership Matters Now

Three forces reshape the role of the security executive. Boards ask for plain answers about exposure and resilience, customers scrutinise incident handling, and scarce specialist talent pushes more work to managed providers and cloud suppliers. A function that sets a clear direction earns funding and trust; one that reports only tool counts loses influence and reacts to every crisis. The course draws on the NIST Cybersecurity Framework 2.0 NIST CSF 2.0, whose Govern function frames executive accountability, and on ISO/IEC 27001:2022 for the information security management system.

Who Gains Most from Information Security Leadership

- Executives accountable for the security strategy and its alignment with business goals
- Deputies who run the security operating model and its daily priorities
- Heads of security who prepare investment cases and defend the security budget
- Leaders who report cyber exposure to boards, audit committees and regulators' liaison teams
- Security leaders who oversee managed service providers and critical suppliers

A security leadership team that attends with its deputies gains most, because it leaves with one shared roadmap and one language for the board.

Information Security Leadership Capabilities

Participants move from running controls to steering a function, turning technical exposure into fundable choices.

- Design a security strategy anchored in business objectives and risk appetite — executive committee
- Build a security operating model with clear roles, sourcing and escalation — chief executive and peers
- Calculate and present investment cases in terms of reduced exposure — chief financial officer
- Communicate security posture through concise board narratives and metrics — board and audit committee
- Specify contractual security expectations and oversight for suppliers — procurement and vendor owners
- Lead crisis decisions and stakeholder messaging during a major incident — crisis management team

Key Information Security Leadership Terms

- Risk appetite — the cyber exposure leaders are willing to accept to pursue their objectives.
- Security operating model — the arrangement of people, processes, sourcing and reporting lines through which the security function delivers its services.
- Key risk indicator — a measure that signals rising exposure early enough for executives to act.
- Board security narrative — a short, non-technical account of posture, trends and decisions needed, written for directors.
- Third-party security assurance — the evidence an organisation gathers that suppliers protect its data and services as agreed.
- Crisis command structure — the predefined roles and decision rights used to lead an organisation through a severe incident.

Information Security Leadership Day by Day

Day 1: The Security Executive's Mandate

- CISO Role Archetypes — Choosing Between Guardian, Advisor and Business Enabler
- NIST CSF 2.0 Govern Function — Setting Executive Accountability for Cyber Risk
- Business Context Mapping — Linking Crown-Jewel Assets to Revenue Streams
- Risk Appetite Statements — Agreeing Tolerable Exposure with the Executive Team
- Stakeholder Influence Map — Prioritising Relationships Across the Leadership Group

Day 2: Strategy and Operating Model

- Security Strategy Canvas — Translating Business Goals into Multi-Year Priorities
- ISO/IEC 27001:2022 Management System — Structuring Policy, Ownership and Review
- Sourcing Options Analysis — Balancing In-House, Managed and Hybrid Services
- Security Team Design — Defining Roles, Career Paths and Succession
- Talent Retention Levers — Keeping Scarce Specialists in a Competitive Market

Day 3: Funding, Metrics and Board Reporting

- Investment Case Structure — Framing Spend as Reduced Loss Exposure
- Budget Prioritisation Matrix — Ranking Initiatives by Risk Reduction per Effort
- Key Risk Indicators — Selecting Measures Directors Can Act Upon
- Board Security Narrative — Presenting Posture Without Technical Jargon
- Audit Committee Questions — Preparing Evidence for Challenging Scrutiny

Day 4: Suppliers and Major Incidents

- Supplier Tiering Model — Focusing Assurance Effort on Critical Providers
- Contractual Security Clauses — Securing Notification, Audit and Exit Rights
- Crisis Command Structure — Assigning Decision Rights During Severe Incidents
- Executive Tabletop Exercise — Testing Leadership Choices Under Time Pressure
- Crisis Communication Plan — Briefing Staff, Customers, Media and Directors

Day 5: Practising the Security Leadership Roadmap

- Mandate and Appetite Review — Confirming Strategic Anchors from Day One
- Operating Model Choices — Selecting Sourcing and Team Design Options
- Metrics and Funding Pack — Combining Indicators with the Investment Case
- Peer Challenge Panel — Stress-Testing Assumptions Before Executive Presentation
- Security Leadership Roadmap — Finalising Priorities, Owners and Milestones

Applying Information Security Leadership After the Course

- Run a risk appetite session with executives and record tolerances for the top three crown-jewel assets.
- Rewrite the next board report as a one-page narrative with four key risk indicators.

Information Security Leadership Questions FAQ

What is information security leadership and why does it matter now?

It is the discipline of running security as a business function, with strategy, funding and accountability. It matters now because boards treat cyber exposure as an enterprise risk and expect security leaders to explain it in business terms.

Which roles gain most from information security leadership for CISOs?

Chief information security officers, their deputies and heads of security gain most. Leaders newly promoted from technical roles benefit strongly, since the course focuses on influence, funding and board communication rather than tools.

How does information security leadership differ from an information security management course?

Leadership focuses on executive decisions such as strategy, budget, talent and crisis command. A management system course centres on implementing and auditing controls, whereas here you decide direction and secure sponsorship for it.

What do you bring back from information security leadership for CISOs?

You bring back a security leadership roadmap drafted on a case organisation. It links risk appetite, operating model, funding and metrics, ready to tailor and present to your own executive team.

Information Security Leadership: The Way Forward

The security leadership roadmap first informs the funding decision at the next budget round. The CISO owns it, the executive team sponsors its priorities, and the board uses its indicators to track progress. After its first use, revisit whether the chosen key risk indicators actually changed executive decisions, and retire any measure that drew no action.