JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Advanced ISMS Implementation and Operation Training Course

**jupiterprime.uk**

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

# Advanced ISMS Implementation and Operation Training Course

ISMS Implementation and Operation is a 2-week advanced training course for information security managers, ISMS owners and compliance leads who must take an information security management system from scope statement to steady running, and it ends with a phased ISMS implementation plan. Customers and partners now ask for proof of a working ISMS before they share sensitive information, so an untested system costs contracts. Jupiter Prime Training offers this course for the people who keep that system alive.

## Why ISMS Implementation and Operation Matters Now

Three forces push the ISMS from paperwork to daily practice: clients and supply chain partners who demand evidence of operating controls in tenders and contracts, cloud and outsourced services that blur where an organisation's information boundary sits, and auditors who now test whether controls run consistently rather than whether policies exist. An organisation that operates its ISMS well finds problems through its own monitoring; one that treats it as a certificate project finds them through incidents. The course rests on ISO/IEC 27001:2022, the international standard for information security management systems, including its Annex A control set.

## Who Gains Most from ISMS Implementation and Operation

- ISMS owners who define scope, objectives and the statement of applicability
- Information security managers who select, implement and monitor Annex A controls
- Compliance leads who map contractual and legal security requirements onto the ISMS
- Internal auditors who plan and report audits against the management system
- IT service managers who run the operational controls the ISMS depends on

A security function that sends its ISMS owner, control owners and internal auditor together gains most, because each sees how their part of the cycle feeds the others.

## ISMS Implementation and Operation Capabilities

Participants leave able to scope, build and run an ISMS that produces its own evidence and improves between audits.

- Specify ISMS scope, boundaries and interfaces with outsourced services — top management approval
- Build an information asset inventory with classification and ownership — asset owners and data stewards
- Assess information security risks and choose treatment options — risk owners and the security committee
- Design a statement of applicability that justifies each Annex A control decision — auditors and certification bodies
- Test control effectiveness through metrics and internal audit — management review

- Apply corrective action and continual improvement routines — ISMS owner and process owners

## Key ISMS Implementation and Operation Terms

- Information security management system — The policies, processes, roles and controls an organisation uses to protect the confidentiality, integrity and availability of its information.
- Statement of applicability — A document listing every Annex A control, whether it is applied, and the justification for each inclusion or exclusion.
- Risk treatment — The choice to modify, retain, avoid or share an information security risk, recorded with the controls that will deliver it.
- Annex A — The reference set of information security controls in ISO/IEC 27001:2022, grouped into organisational, people, physical and technological themes.
- Management review — A scheduled meeting where top management examines ISMS performance, audit results and changes, and decides on improvements and resources.
- Nonconformity — A failure to meet a requirement of the standard or of the organisation's own ISMS, which needs correction and root cause action.

## ISMS Implementation and Operation Day by Day

## Day 1: The Case for a Living ISMS

- ISO/IEC 27001:2022 Clause Structure — Management System Requirements Versus Controls
- Plan-Do-Check-Act Cycle — Rhythm of ISMS Operation
- Stakeholder and Interested Party Mapping — Security Expectations to Satisfy
- Gap Assessment Against the Standard — Starting Effort and Priorities
- Leadership Commitment Evidence — Roles Top Management Must Play

## Day 2: Scoping and Context

- Scope Statement Drafting — Sites, Services and Exclusions
- Internal and External Issues Analysis — Factors Shaping Security Objectives
- Interfaces with Cloud and Outsourced Providers — Boundary Responsibilities
- Information Security Policy Framework — Top-Level Direction and Topic Policies
- Security Objectives and Measures — What the ISMS Must Achieve

## Day 3: Information Assets and Classification

- Asset Inventory Methods — Information, Systems, People and Suppliers
- Asset Ownership Assignment — Accountability for Protection Decisions
- Classification Scheme Design — Labels and Handling Rules
- Acceptable Use and Return of Assets — Staff Joiner and Leaver Controls
- Configuration and Asset Tooling — Keeping the Inventory Current

## Day 4: Risk Assessment Methodology

- Risk Criteria and Acceptance Levels — Consistent and Repeatable Results
- Asset-Based Versus Scenario-Based Methods — Choosing the Approach
- Threat and Vulnerability Identification — Likelihood Inputs
- Impact Scales for Confidentiality, Integrity and Availability — Consequence Ratings
- Risk Owner Sign-Off — Accountability for Residual Exposure

## Day 5: Risk Treatment and the Statement of Applicability

- Treatment Option Selection — Modify, Retain, Avoid or Share
- Annex A Control Mapping — Linking Each Risk to Safeguards
- Statement of Applicability Justifications — Inclusions and Exclusions Auditors Accept
- Risk Treatment Plan Scheduling — Owners, Resources and Deadlines
- Residual Risk Acceptance Records — Formal Approval by Risk Owners

## Day 6: Organisational and People Controls

- Roles, Segregation of Duties and Contacts — Clear Security Responsibilities
- Supplier Security Agreements — Contract Clauses and Monitoring
- Screening, Terms and Disciplinary Process — People Lifecycle Controls
- Awareness and Competence Records — Evidence of Trained Staff
- Information Security Incident Process — Reporting, Response and Learning

## Day 7: Physical and Technological Controls

- Secure Areas and Equipment Protection — Physical Perimeter Decisions
- Access Control and Identity Management — Least Privilege in Practice
- Logging, Monitoring and Threat Intelligence — Detection Coverage
- Secure Configuration and Vulnerability Handling — Patch and Hardening Cadence
- Backup, Redundancy and Data Leakage Prevention — Availability and Disclosure Safeguards

## Day 8: Documentation and Operational Evidence

- Documented Information Control — Versioning, Approval and Retention
- Procedure and Work Instruction Design — Usable Guidance for Operators
- Security Metrics and Dashboards — Measuring Control Effectiveness
- Change Management Integration — Security Checks in IT Changes
- Healthcare and Logistics Implementation Cases — Sector Lessons

## Day 9: Internal Audit and Management Review

- Internal Audit Programme Planning — Coverage Across Clauses and Controls
- Audit Evidence Sampling and Interviews — Testing Operation Not Paperwork
- Nonconformity Grading and Reporting — Clear Findings for Owners
- Management Review Inputs and Outputs — Decisions on Resources and Change
- Corrective Action and Root Cause Methods — Preventing Recurrence

## Day 10: Practising the ISMS Implementation Plan

- Scope and Context Applied to a Case Organisation — Defensible Boundaries
- Risk Treatment and Applicability Exercise — Control Choices Under Constraint
- Audit Simulation and Findings Response — Readiness for External Assessment
- Continual Improvement Roadmap — Cycle After First Certification
- ISMS Implementation Plan Completion — Phases, Owners and Evidence Milestones

## Applying ISMS Implementation and Operation After the Course

- Run a gap assessment of the current ISMS against ISO/IEC 27001:2022 clauses and present the priority gaps to top management
- Review the statement of applicability with control owners and add a measurable effectiveness check for each applied control

## ISMS Implementation and Operation Questions FAQ

### What is ISMS implementation and operation and why does it matter now?

ISMS implementation and operation is the work of building and running an information security management system that meets ISO/IEC 27001:2022. It matters now because clients and partners ask for evidence of working controls, not just policies, before they trust an organisation with information.

### Which roles gain most from ISMS implementation and operation training?

ISMS owners, information security managers, compliance leads and internal auditors gain most. You benefit if you own the statement of applicability, run controls, or must show auditors that the system works between assessments.

### How does ISMS implementation and operation training differ from an ISO/IEC 27001 awareness course?

It goes beyond explaining requirements to building and running each part of the system. You practise scoping, risk treatment, control selection, internal audit and management review, and leave with a plan for your own organisation rather than an overview.

### What do you bring back from ISMS implementation and operation training?

You bring back a phased plan for implementing or strengthening your ISMS. It sets out scope, risk method, control priorities, audit schedule and evidence milestones, with named owners for each phase.

## ISMS Implementation and Operation: The Way Forward

The ISMS implementation plan first informs which scope boundary and risk method top management approves. ISMS owners steer it, control owners deliver its phases and internal auditors use it to plan coverage. After the first internal audit cycle, revisit the statement of applicability, since audit evidence often shows controls that were applied on paper but not yet operating.