# ISO 27001 Deployment Overview

Summarising the implementation path

# Deployment Stages

The ISO 27001 implementation process involves five key stages.

Each stage ensures the development, execution, evaluation, and enhancement of an effective Information Security Management System (ISMS).

This guide provides a brief overview so you can familiarise yourself with their purpose.

1) Initiation

2) Planning

3) Implementation

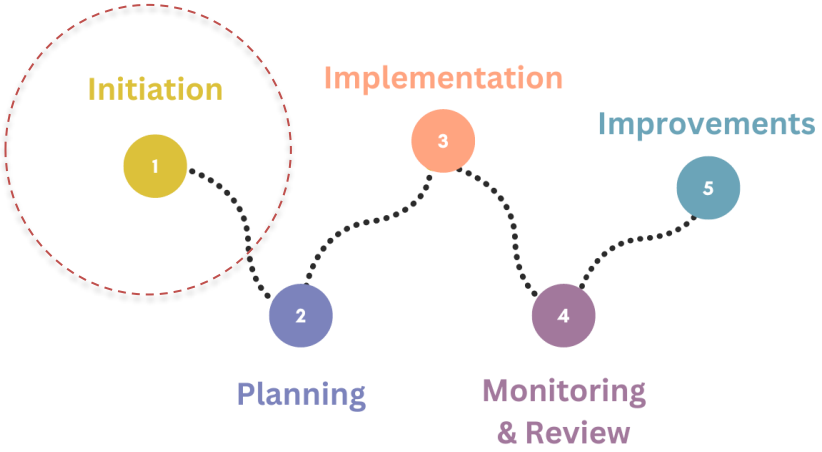
4) Monitoring & Review

5) Continuous Improvement

# Step 1: Initiation

The initiation phase builds the foundations and blueprint for your ISMS.

Here, we establish a project plan and steering group, define the ISMS scope, develop an information security policy, assign roles and responsibilities, and set objectives to guide the deployment process.

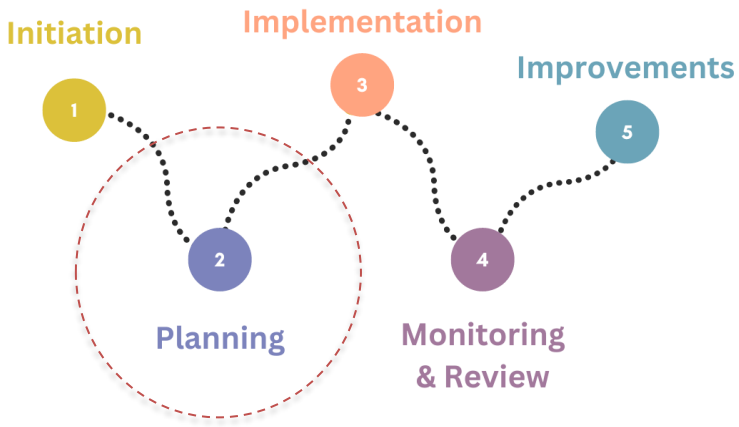



| | |
|---|---|
| Establish | A Project Plan |
| Assemble | A Steering Group |
| Define | The ISMS |
| Develop | An Information Security Policy |
| Document | ISMS Roles and Responsibilities |
| Set | ISMS Objectives |

# Step 2: Planning

The planning phase is about defining your organisation's approach to risks.

The stage involves defining a risk assessment methodology, identifying and evaluating risks, determining treatment options, and updating the Statement of Applicability (SoA) to reflect necessary controls based on the risk assessment findings.




| | |
|---|---|
| Define | Define Risk Methodology |
| Identify | Identify Risks |
| Analyse & Evaluate | Analyse & Evaluate Risks |
| Determine | Determine Risk Treatment Options |
| Update | Update Statement of Applicability (SoA) |

# Step 3: Implementation

The implementation phase is about putting the plan into action.

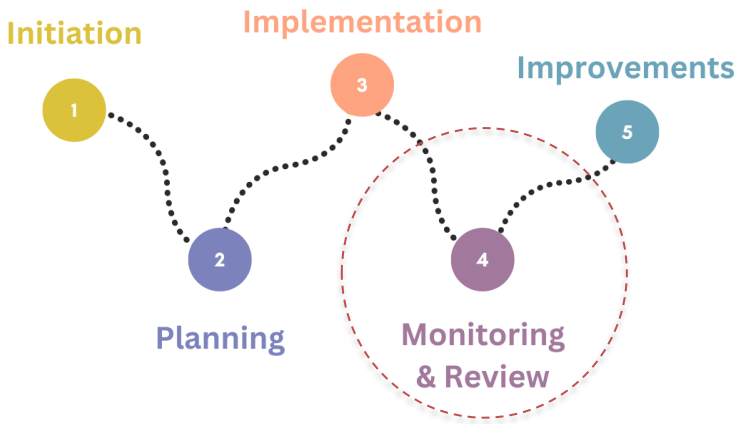
Here we build the resource plan, document necessary policies and procedures, implement information security controls, conduct awareness campaigns, and provide training to ensure all staff understand ISMS policies and responsibilities.


| | |
|---|---|
| Create | A Resource Plan |
| Document | Policies & Procedures |
| Implement | Controls |
| Conduct | An Awareness Campaign |
| Provide | Training |

# Step 4: Monitoring & Review

This phase monitors ISMS performance.

Here, we set up a framework to conduct management reviews and perform internal audits to ensure compliance with ISO 27001 requirements, documenting findings to identify non-conformities and areas for improvement.

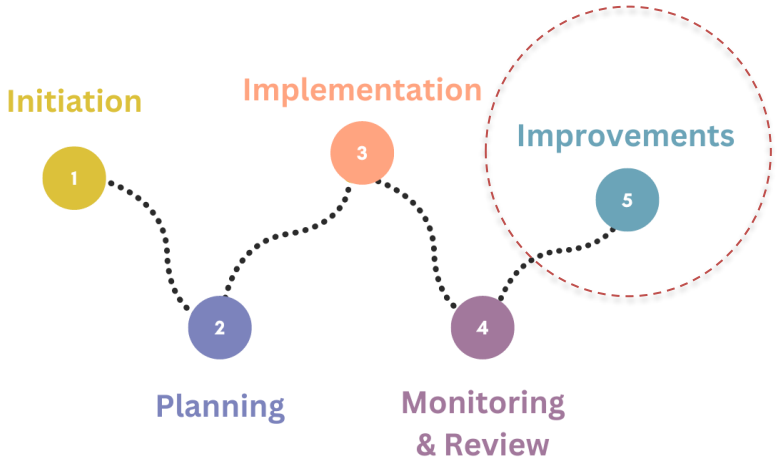



| | |
|---|---|
| Monitor & Measure | ISMS Performance |
| Hold | Management Reviews |
| Conduct | Internal Audits |

# Step 5: Continuous Improvement

The stage ensures the ISMS evolves and remains effective in meeting organisational needs.

Continuous improvement addresses non-conformities where the ISMS operations deviate from expectations and implements enhancements based on performance reports, management reviews, and audit findings.




| | |
|---|---|
| Create | An Improvement Plan |
| Maintain | Non-Conformities Log |