10 Steps to
ISO 27001 Certification

Implementation project

Starting right is the first step to success, ensure you have management buy-in and an idea of how you're going to complete the project with what resources and tools. Perform an initial gap analysis to identify your starting point.

Scope, Context and Interested parties

Define what needs to be in the "scope" of the management system, and have this documented. Identify your interested parties, both internal and external.

ISMS policy, roles and responsibilities

Create an ISMS Policy and define the roles in your management system and what they are expected to do. Identify any immediate training needs for the people involved.

ISMS risk, opportunities and security objectives

Define a risk assessment process and carry it out to produce a risk treatment plan. Set your objectives for the ISMS.

Competence, awareness and communication

Evaluate any competency gap and how it might be filled. Put in place an awareness training programme and define how you will communicate to interested parties about the ISMS.

Documented information

Decide how documented information will be created and controlled within the ISMS. Develop a set of policies, procedures and other relevant documents to support the ISMS and its operation.

Operational

Ensure you have the ISMS processes in place and that your risk treatment plan is delivering results.

Performance review

Put an internal audit programme in place, define how nonconformities will be addressed and hold a management review.

Update gap assessment plan and actions

Revisit the gap assessment to see what still needs to be done, and by whom. Check that you have all of the necessary documentation in place.

Plan for your certification

Choose a certification body to carry out your audits, and check that everything is ready for their visits.

CERTIKIT
Compliance made easy

certikit.com
enquiries@certikit.com