

• GOVERNANCE, RISK & COMPLIANCE

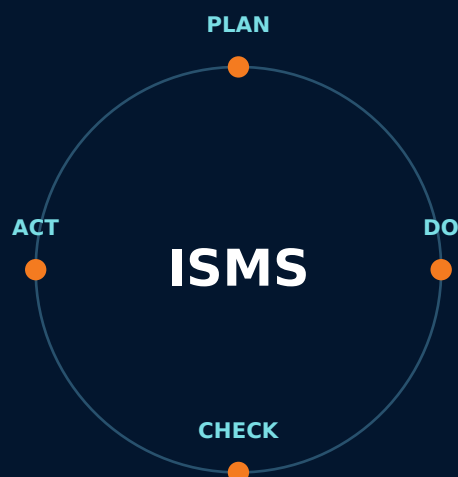
ISO 27001

Implementation & Certification Support

Protect your information.
Build lasting confidence.

A practical, risk-based path to ISO/IEC 27001:2022 readiness, from gap assessment and implementation to independent certification audit support.

- 01 Assess**
Understand your starting point.
- 02 Implement**
Build controls that fit your risks.
- 03 Improve**
Make security sustainable.



TRUSTED SECURITY ADVISOR

Turn requirements into resilience.

• 01 / SERVICE OVERVIEW

Information security. Built around your business.

ISO/IEC 27001:2022 provides a framework for establishing, implementing, maintaining and continually improving an information security management system (ISMS). Cyber360 helps you translate its requirements into practical governance, processes and controls that fit your organisation.

Expert guidance

Clear advice from initial scoping to certification audit preparation.

Tailored approach

An ISMS shaped around your business context, information assets and risk profile.

Sustainable security

Defined ownership, repeatable processes and continual improvement.

• 02 / BUSINESS VALUE

Why invest in an ISMS?

01

Stronger security

Identify information risks and implement proportionate controls to protect critical assets.

02

Commercial confidence

Support tenders and customer assurance where ISO 27001 certification is requested.

03

Compliance alignment

Reuse relevant evidence across contractual and regulatory obligations; separate requirements still apply.

04

Operational clarity

Establish clear responsibilities, documented processes and measurable security objectives.

05

Stakeholder trust

Prepare for independent assessment of the ISMS within its defined certification scope.

06

Incident readiness

Strengthen prevention, response and improvement processes to manage the impact of incidents.

RISK-BASED. BUSINESS-ALIGNED.

More than a documentation exercise.

We focus on how security operates in practice: people, processes, technology and governance, supported by evidence and a cycle of continual improvement.

• 03 / OUR APPROACH

Your path to certification readiness.

Seven stages, tailored to your scope, maturity and implementation priorities.

01 Gap analysis & scoping

Assess current arrangements against ISO/IEC 27001:2022 requirements and relevant Annex A controls. Define the ISMS scope and prioritise gaps.

02 ISMS framework development

Establish a framework aligned with your business context, stakeholders, objectives, governance and operational environment.

03 Risk assessment & treatment

Develop an ISO 27005-aligned methodology, risk register, ownership, acceptance criteria and prioritised treatment plans.

04 Security controls implementation

Work with your team to implement proportionate organisational, people, physical and technological controls addressing identified risks.

05 Documentation & processes

Create practical policies, procedures, work instructions and records that support consistent operation and evidence of the ISMS.

06 Internal audit & improvement

Support objective internal audits, management reviews, performance measures and corrective actions to evaluate and improve the ISMS.

07 Certification audit support

Prepare for Stage 1 and Stage 2 audits, coordinate evidence and communications, and support responses to findings from the certification body.

INDEPENDENT CERTIFICATION

Cyber360 provides implementation and advisory support. Certification is awarded by an independent certification body following its assessment; the outcome is not guaranteed.

• 04 / WHAT YOU RECEIVE

Practical outputs. Clear ownership.

Deliverables are tailored and confirmed within your agreed engagement scope.

01 Gap assessment report

A structured view of gaps, maturity and priorities against the applicable requirements and controls.

02 ISMS documentation suite

Policies, procedures, work instructions and records tailored to your organisational context.

03 Risk assessment framework

Risk methodology, acceptance criteria, assessment tools, risk register and treatment plans.

04 Statement of Applicability

Applicability decisions for the 93 Annex A reference controls, with rationale and implementation status.

05 Implementation roadmap

Agreed milestones, responsibilities, resource needs and a prioritised plan for closing identified gaps.

06 Internal audit programme

Audit schedules, checklists, reporting templates and guidance to support ongoing assurance.

07 Certification readiness support

Audit preparation, evidence coordination and support addressing Stage 1 and Stage 2 findings.

08 Post-certification support

A 12-month support plan can include surveillance audit preparation, quarterly reviews and advisory support, as agreed.

• KEEPING YOUR ISMS EFFECTIVE

Certification is a milestone. Continual improvement is the goal.

Maintain ownership of controls, review changing risks and use audits and management reviews to keep the ISMS relevant as your business evolves.

Start your ISO 27001 journey.

cyber360.co

info@cyber360.co

UK +44 20 3286 1927

UAE +971 55 768 7199