SAPPHIRE™

# ISO 27001 Consultancy Service Definition

**Classification**: Public

# Contents



# Proprietary Notice

# Overview

ISO 27001 is the global best practice standard for information security. Gaining compliance with or Certification to ISO 27001 proves that your organisation takes the confidentiality, integrity and availability of its information seriously.

The ability to respond quickly to information security breaches or incidents is one of the key goals of ISO 27001. Ensuring the capability to minimise the opportunity for incidents to occur will also give your organisation a major advantage in service resilience and will help build confidence in your ability to handle information in a secure manner.

Sapphire offers a modular programme of consultancy. Sapphire's methodology will enable the development of a robust Information Security Management System (ISMS).

# Functional and Non-Functional Detail

ISO 27001 is the de-facto international standard on establishing, operating and maintaining an Information Security Management System (ISMS). The standard includes both specific mandatory processes and policies which must be adhered to in order to gain formal Certification. There are 93 information security control objectives across 4 themes:

- Organisational Controls
- People Controls
- Physical Controls
- Technological Controls

The ISMS must be fully integrated across the business with a working ISMS is in place. A typical document set from the Information Management System will include, but not limited to the following:

## Scope & Statement of Applicability

- ISO 27001: Scope Statement
- ISO 27001: Statement of Applicability

## Risk Management Policy & Information Assets

- Threat Intelligence Policy
- Risk Management Policy
- Information Assets and Risk Register

## Strategic Policies

- Executive Oversight Guide
- Strategic Objectives
- Corporate IS Policy
- Security Objectives Policy
- Communications Policy
- Roles/Responsibilities Policy

## Tactical & Operational Guidance

- IS Manual
- Personal IS Policy
- Access Control Policy
- Cryptographic Controls Policy
- IT Policies & Procedures (including DLP)
- HR Policies
- Facilities Policies
- Information Classification and Handling Policy
- Information Transfer Policy
- Change Management Policy
- Secure Development & System Engineering Principles Policy
- Supplier Relationship Policy
- Supplier Relationship Procedure
- Third Party Questionnaire

## Incident Management & Business Continuity Plan

- Incident Management Process
- Forensic Readiness Policy
- Business Continuity Plan

## On-going Compliance Policies & Procedures

- Data Protection Policy
- Data Retention & Erasure Policy
- Privacy Impact Assessment Guidance
- Project Management Security Guidance

- Management Review Policy
- Corrective Action Policy
- Effectiveness Review Policy
- Document Control and Control of Records Policy

## Internal Audit Documentation

- Internal Audit Policy
- Internal Audit Programme

The typical phases completed as part of ISO 27001 is:

- Current State Analysis (Gap Analysis)
- Risk Assessment and Management
- Security Improvement Plan (policies and procedures document set)
- Information Security Awareness Education and Training
- Mock Compliance

## Self Versus Formal Certification

An organisation can claim self-compliance to the standard. This means it operates an ISMS (Information Security Management System), but it is not intending to gain formal Certification. An organisation may still be subject to an audit by customers or clients who have imposed a requirement to be compliant, through a contractual clause or during the tender process.

Operating an ISMS and claiming self-compliance provides a common basis for developing organisational security standards, an effective security management practice and confidence in inter-organisational dealings.

Formal Certification is awarded by independent third-party Certification bodies. By being certified an organisation is subject to continual six-monthly surveillance audits and re-Certification audits every 3 years. This ensures the organisation is continually monitoring and improving its ISMS in order to maintain its Certification status.

## Benefits

By having formal documented ISMS which has been independently assessed, an organisation can demonstrate to its customers and clients that it is committed to security and has the ability to handle information in a secure manner. Equally customers and clients gain confidence in the organisation thereby increasing trust in its brand and/or image.

The reputation of ISO and the Certification against the internationally recognised ISO 27001:2022 security standard enhances an organisations' credibility and may lead to an increase in its market share.

## Accreditation or Certification?

Often there is confusion between Accreditation and Certification when discussing the audit.

Accreditation bodies regulate Certification bodies. Each country has its own Accreditation body. The Accreditation body in the United Kingdom is UKAS, the United Kingdom Accreditation Service. This body issues Accreditations to Certification bodies for each standard that the Certification body wishes to offer Certification services for.

The Certification bodies therefore are accredited by UKAS with the power to issue Certifications.

# Sapphire's Certifications and Associations