COGNISYS

COMPLIANCE

ISO 27001

ISO 27001 is the international standard for Information Security Management Systems.

ISO 27001 sets the global benchmark for a risk-based approach to cyber security management. It establishes a comprehensive framework to ensure effective information security, cybersecurity, and privacy protection.

An ISO 27001 ISMS helps to make sure information is always appropriately protected to assist with the preservation of:

- Confidentiality – ensuring that access to information is appropriately authorised
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – ensuring authorised users have access to information when required

Why ISO 27001?

This testing is designed to assess security posture against best practices and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered. Improved information security: By implementing the controls outlined in the standard, your organisation will better protect its sensitive data and systems from cyber threats and other security risks.

Increased customer trust

ISO 27001 certification demonstrates to customers and clients that an organisation takes information security seriously and is committed to protecting its data.

Enhanced compliance

Many industries and sectors have regulatory requirements related to information security. ISO 27001 certification helps meet these requirements and demonstrate compliance.

Competitive advantage

In some cases, clients may only do business with organisations that have demonstrated their commitment to information security through ISO 27001 certification.

Improved risk management

The risk assessment and management process required for ISO 27001 certification can help an organisation identify and prioritise potential security risks and implement controls to mitigate them.

Improved business continuity

By implementing the controls outlined in the standard, an organisation can improve its ability to continue operating in the event of a security incident or other disruptive event.

ISO 27001 services

- GAP Analysis
- Development & Implementation
- Internal Auditing
- External Auditing (Stage 1, Stage 2, Surveillance)
- Management and maintenance (Continual improvement)

Why Cognisys?

There are several reasons why an organisation should choose to use Cognisys to help with the development and implementation of an ISO 27001 ISMS:

Expertise

Our team has extensive experience in ISO 27001 and holds all the relevant qualifications. We provide valuable expertise and guidance throughout the process of implementing an ISO 27001-compliant ISMS. We help the organisation understand the requirements of the standard and how to effectively implement them.

Objectivity

We provide an objective perspective and help identify potential weaknesses or gaps in the organisation's current security practices.

Time and resource savings

Developing and implementing an ISMS can be a time-consuming and resource-intensive process. We help streamline the process and ensure that it is completed efficiently.

Independent verification

We provide independent verification of the organisation's ISMS, which is helpful in demonstrating compliance to regulatory bodies or clients.

Ongoing support: We provide ongoing support to help the organisation maintain its ISMS and ensure ongoing compliance with the standard.

Reporting

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations.

BACK TO CONTENTS