responsiv
simple · effective · distinctive

www.responsiv.co.uk

ISO 27001 CERTIFICATION: AN INTRODUCTION

AT A GLANCE

7 Steps for a Successful ISO 27001 Risk Assessment

- Define the chosen risk assessment methodology and focus business areas
- Compile list of information assets within the scoped business area
- Identify threats and vulnerabilities
- Evaluate risks
- Mitigate the risks
- Compile risk reports
- Review, monitor, and audit

BENEFITS

Business Opportunities

Build trust with customers by demonstrating effort and actions to protect their data.

Ongoing Awareness

Audits are regularly conducted including tests of security, incident management, business continuity, and security monitoring, ensuring organisations are continuously aware of their data risks and governance.

Greater Visibility of Threats

The systematic risk assessments aid in identifying vulnerabilities that require mitigative action to secure.

READ MORE

CHALLENGE

Organisations are faced with regulatory compliance demands, customer expectations to keep confidential data secure, and increased risk associated with cyber attacks.

This has meant organisations have started to prioritise effective measures against cyber security threats. One of these measures is implementing and becoming ISO 27001 certified. ISO 27001 is an international standard focusing on information security.

In today's market, organisations that choose not to implement the framework risk losing out on new business from customers who require the certification as part of their third-party risk management strategy.

FRAMEWORK

The ISO 27001 framework is a set of requirements for defining, operating, implementing, and improving Information Security Management Systems (ISMS).

It is mainly concerned with identifying risk and addressing them through control measures. The focus is to protect the confidentiality, availability, and integrity of data.

The process of becoming ISO 27001 certified is long and costly, but allows organisations the opportunity to assess, understand, and protect valuable information. This process is reiterative, and requires reassessment over time to ensure measures are still being taken to maintain data security and governance.

Achieving ISO 27001 compliance provides evidence to customers and partners that their data is safeguarded and that their third-party risk is reduced.

Who Needs ISO27001?

Becoming ISO 27001 certified is a business choice and should be properly considered before starting the journey. This choice includes scoping the areas of business you want to get ISO certified.

You may consider becoming certified if you are:

- A company dealing with sensitive employee and customer data
- A company that must comply with regulatory and legal requirements such as GDPR
- A third-party service provider that handles sensitive information on behalf of clients