# SERVICE DESCRIPTION
# ISO 27001

LexQ Certifications

QUALIFYING QUALITY

# ISO 27001

## ISO/IEC 27000 FAMILY - INFORMATION SECURITY MANAGEMENT SYSTEMS

Information is a valuable asset that can make or break your business. When properly managed it allows you to operate with confidence. Information security management gives you the freedom to grow, innovate and broaden your customer-base in the knowledge that all your confidential information will remain that way.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

## WHAT IS AN ISMS?

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Internationally recognized ISO/IEC 27001 is an excellent framework which helps organizations manage and protect their information assets so that they remain safe and secure. It helps you to continually review and refine the way you do this, not only for today, but also for the future. That's how ISO/IEC 27001 protects your business, your reputation and adds value.

It can help small, medium and large businesses in any sector keep information assets secure.

## WHY IS ISO 27001 SO IMPORTANT?

The business benefits from ISO 27001 certification are considerable. Not only do the standards help ensure that a business' security risks are managed cost-effectively, but the adherence to the recognized standards sends a valuable and important message to customers and business partners: this business does things the correct way. ISO 27001 is invaluable for monitoring, reviewing, maintaining and improving a company's information security management system and will unquestionably give partner organizations and customers greater confidence in the way they interact with your business.

## WHERE DO YOU SEE INFORMATION SECURITY HEADING INTO THE FUTURE?

"Anything that can be digitized is being digitized, so access to information and anything that is connected presents far greater risk to society than ever before.
As long as there is a dependence on technology to live, there will always be malicious, accidental and other ways to cause negative impacts. Security is a byproduct of risk management. Security in the context of this conversation is about shifting the cyber risks in your favour – InfoSec must become part of your everyday personal and professional lives just like locks on your doors. Live it, breath it."

## BENEFITS OF ISO 27001

**1. Compliance**
It might seem odd to list this as the first benefit, but it often shows the quickest "return on investment" – if an organization must comply to various regulations regarding data protection, privacy and IT governance (particularly if it is a financial, health or government organization), then ISO 27001 can bring in the methodology which enables to do it in the most efficient way.

## 2. Marketing edge

In a market which is more and more competitive, it is sometimes very difficult to find something that will differentiate you in the eyes of your customers. ISO 27001 could be indeed a unique selling point, especially if you handle clients' sensitive information.

## 3. Lowering the expenses

Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees.

The truth is, there is still no methodology and/or technology to calculate how much money you could save if you prevented such incidents. But it always sounds good if you bring such cases to management's attention.

## 4. Putting your business in order

This one is probably the most underrated – if you are a company which has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain information assets, who has to authorize access to information systems etc.

ISO 27001 is particularly good in sorting these things out – it will force you to define very precisely both the responsibilities and duties, and therefore strengthen your internal organization.

To conclude – ISO 27001 could bring in many benefits besides being just another certificate on your wall. In most cases, if you present those benefits in a clear way, the management will start listening to you.

# ISO 27001

## WHAT VALUE DOES ISO 27001 CERTIFICATION ADD TO A BUSINESS?

“Certification is fundamentally about providing trust and confidence – and these can provide a competitive edge. In today’s world, our customers, business partners and shareholders want to be sure that you’re not putting them or their businesses at risk by not having appropriate safeguards in place around information and technology enabled business assets.

Boards want this confidence; management wants this confidence; and certification is a solid way of showing that you have invested and continue to invest to maintain appropriate levels of security based on acknowledged risks.”

## THREE STEPS TO CERTIFICATION

**Application** for registration is made by completing the Quote Request Form for the desired standard. This form provides information about your organization so we can accurately define the scope of certification and the assessment duration.

**Assessment** is undertaken by Lex Q against the specific requirements of your chosen Standard. This consists of two mandatory visits that form the Initial Certification Audit (explained below). Please note that you must be able to demonstrate that your management system has been fully operational for a minimum of three months and has been subject to a management review and full cycle of internal audits.

**Certification** is issued by Lex Q on successful completion of the Stage 2 assessment. Certification is maintained through a program of annual surveillance audits and a three yearly recertification audit.

# ISO 27001

## INITIAL CERTIFICATION AUDIT

## STAGE 1

The purpose of this audit is to confirm that your organization is ready for full assessment.

**The assessor will:**

- Confirm that the management system conforms to the requirements of the standard.
- Confirm its implementation status.
- Confirm the scope of certification.
- Check legislative compliance.
- Produce a report that identifies any non-compliance or opportunities for improvement and agree a corrective action plan if required.
- Produce an assessment plan and confirm a date for the Stage 2 assessment visit

## STAGE 2

The purpose of this audit is to confirm that the management system fully conforms to the requirements of the chosen Standard in practice.

**The assessor will:**

- Undertake sample audits of the processes and activities defined in the scope of certification.
- Document how the system complies with the standard by using objective evidence.
- Report any non-compliances or opportunities for improvement.
- Produce a surveillance plan and agree a date for the first annual surveillance visit.

If the assessor identifies any major non-conformances, certification cannot be issued until correction and corrective action is taken and verified. Accreditation requirements stipulate that if this is not completed within 6 months, then certification cannot be recommended without a further stage 2 assessment.

## SURVEILLANCE AUDIT

Surveillance audits are undertaken periodically to ensure that compliance to the chosen Standard is maintained throughout the three year certification cycle.

**The frequency and duration of surveillance is dependent on factors including:**

- Size and structure of organization.
- Complexity and risk of activities
- Number of management systems standards included in the scope of certification