



IT Governance

**ISO/IEC 27001:2013 ISMS  
Implementation**

Service description

Protect • Comply • Thrive

## **100% guaranteed ISO 27001 certification with the global experts**

With the [IT Governance ISO 27001 Implementation Consultancy](#), we facilitate implementing ISO 27001 in your organisation right up to certification. This bespoke consultancy service is usually delivered in a traditional, face-to-face, format, but may also be delivered online utilising the IT Governance mentor and coach\* consultancy format. To learn more about the types of consultancy available, please see the IT Governance consultancy section below.

### **Payment options**

Our consultancy team will arrange a scoping session to assess your organisation's needs and supply you with a quote that transparently outlines all the costs of your ISO 27001-compliant ISMS implementation project. A payment plan will be agreed with you up front. This package does not include certification fees, which are paid directly to the certification body.

### **Resource requirements**

Whichever type of consultancy service you choose, you will need to provide essential information for the project to proceed according to schedule and to fulfil its objectives. It is essential that your staff give any requests the appropriate priority and an outline implementation plan for the project will be provided in a professional services agreement in advance, together with an indication of the level of management time that is likely to be required to ensure ISMS development tasks are carried out effectively.

### **Applicability**

This consultancy service is suitable for any size of organisation, in any industry or sector and has been specifically designed to be delivered as a face-to-face engagement. It is ideally suited to large, complex organisations that require extensive support to ensure the successful management and execution of their ISMS implementation project.

### **Service description**

A qualified consultant will work with you to ensure all the key activities of setting up a working ISO 27001 ISMS (information security management system) are undertaken appropriately. IT Governance will ensure that the project remains on track, and achieves its objectives, using a combination of mentor and coach, advice and

guidance, and in-house<sub>2</sub> delivery with appropriate oversight to maximise the value of the project's deliverables.

#### **1. Mentor and coach consultancy**

An assigned consultant will advise your internal project team on the key stages of the project, developing answers from first principles to ensure your team acquires the necessary knowledge and understanding. The consultant will also be available by phone and email to handle queries as and when they occur. This typically includes advising on the implementation of specific requirements, ensuring suitable training and awareness is established, and monitoring project progress. The mentor and coach consultancy service will normally be delivered at your site.

#### **2. In-house project management service**

IT Governance will remove the hassle of certain tasks or even run your project by providing a consultant to work for you in-house. This service can be delivered at your site or remotely according to your requirements, and means that IT Governance expertise is always to hand. As our consultants are already trained and experienced in ISO 27001 implementation, there is no need for a member of staff to develop these skills. In addition, our consultants use a consistent, comprehensive methodology, which means that if a new consultant needs to be assigned for any reason, there will be a smooth transition and minimal disruption to the project.

The project will follow IT Governance's popular nine-step methodology for ISMS implementation.

### **1. Project mandate**

IT Governance will collate all information relating to your commitment to proceed with the project, reviewing senior-level objectives in implementing an ISMS, top-level information security goals, and produce a project initiation document (PID) for approval by the appropriate authority.

### **2. Project initiation**

This stage develops the project's objectives, including establishing a project governance structure (e.g. a steering committee or project board), a full project plan and a project risk register to assist in ensuring that both the project and the ISMS succeed in delivering the objectives.

### **3. ISMS initiation**

Laying the foundations of the ISMS at an early stage helps with project management and encourages ownership of the ISMS within the organisation. These early foundations include introducing arrangements for document management, roles and responsibilities, continual improvement of the ISMS, internal and external communication, and ISMS project awareness.

### **4. Management framework**

This stage addresses the critical ISO 27001 requirements relating to organisational context, scope and leadership, and ensures that the ISMS framework is aligned with and supports the delivery of business objectives.

## **5. Baseline security criteria**

Any organisation already has a number of security controls in place. Ensuring these existing security controls meet the requirements of the relevant legislation, regulations and contracts early in the project can provide a significant level of comfort to senior management and helps establish an effective information security stance.

## **6. Risk management**

This stage covers the development of a robust information security risk methodology, an information security risk assessment, and identification of appropriate information security risk treatments. The default approach is an asset-based risk assessment, unless specifically required otherwise. IT Governance will provide a thorough risk assessment, a Statement of Applicability (SoA) and a risk treatment plan.

## **7. Implementation**

The implementation phase addresses both management system processes and information security controls to make sure that the design of the ISMS and operation of its processes are carried out by individuals with proven competence. This includes ensuring staff have an appropriate level of understanding of information security and the ISMS, and their role in supporting its effectiveness. This phase also involves controlling outsourced information security processes.

## **8. Measure, monitor and review**

This phase establishes the performance measurement capability of the ISMS, including its processes and security controls. Key areas include an internal ISMS audit and management review.

## **9. Certification audit**

Before the third-party audit, an IT Governance ISMS auditor will conduct a mock certification audit aimed at identifying any areas for improvement and preparing the organisation for the certification process. Following this, IT Governance will provide support throughout the certification audit to help with any unexpected issues that might arise.

*"Finding the right supplier of consultancy services was the key as far as we were concerned."*

**Carl White, Service Manager, Lanware**

## **Certification success guarantee**

The IT Governance certification guarantee provides assurance that accredited third-party certification will be recommended, subject to the following:

- That the client executes the tasks identified in the project plan agreed at the project initiation stage and as it may be varied afterwards.
- That the project plan may be varied during execution of the project only by express agreement with IT Governance.
- During third-party audits, the client follows all recommendations made by IT Governance.

In the event that certification is not recommended at the first attempt, IT Governance will carry out the remedial work necessary to secure certification at the next attempt and will pay the additional costs due to the selected accredited certification body.

## **Next steps: maintaining your ISMS**

Maintaining a healthy ISMS is a commitment that extends beyond initial certification. Although this bespoke consultancy service will bring you to accreditation, guaranteed, you will need to consider setting aside resources to maintain ongoing compliance with the requirements of ISO 27001. IT Governance will help create an ongoing plan for maintenance of the ISMS, and transfer knowledge and skills to your people throughout the project to enable your organisation to continue meeting compliance targets after the initial implementation period ends.

## **IT Governance consultancy**

IT Governance offers three types of consultancy service, enabling you to get the ideal mix of ISMS support and services that best meet your requirements for each stage of your project and budget:

### **Internal audit**

As well as having extensive practical experience handling ISMS issues, IT Governance also has suitably trained and experienced auditors who can provide independent assurance regarding the fitness for purpose of the ISMS and related arrangements. IT Governance is also able to audit your suppliers on your behalf to provide assurance regarding their information security capabilities and how they align with your requirements. This service is also available as a remotely delivered consultancy service.

## **Contact us now for an obligation-free quote**

Speak to a member of our team to discuss your consultancy requirements by emailing [servicecentre@itgovernance.co.uk](mailto:servicecentre@itgovernance.co.uk) or calling us on +44 (0)845 070 1750.