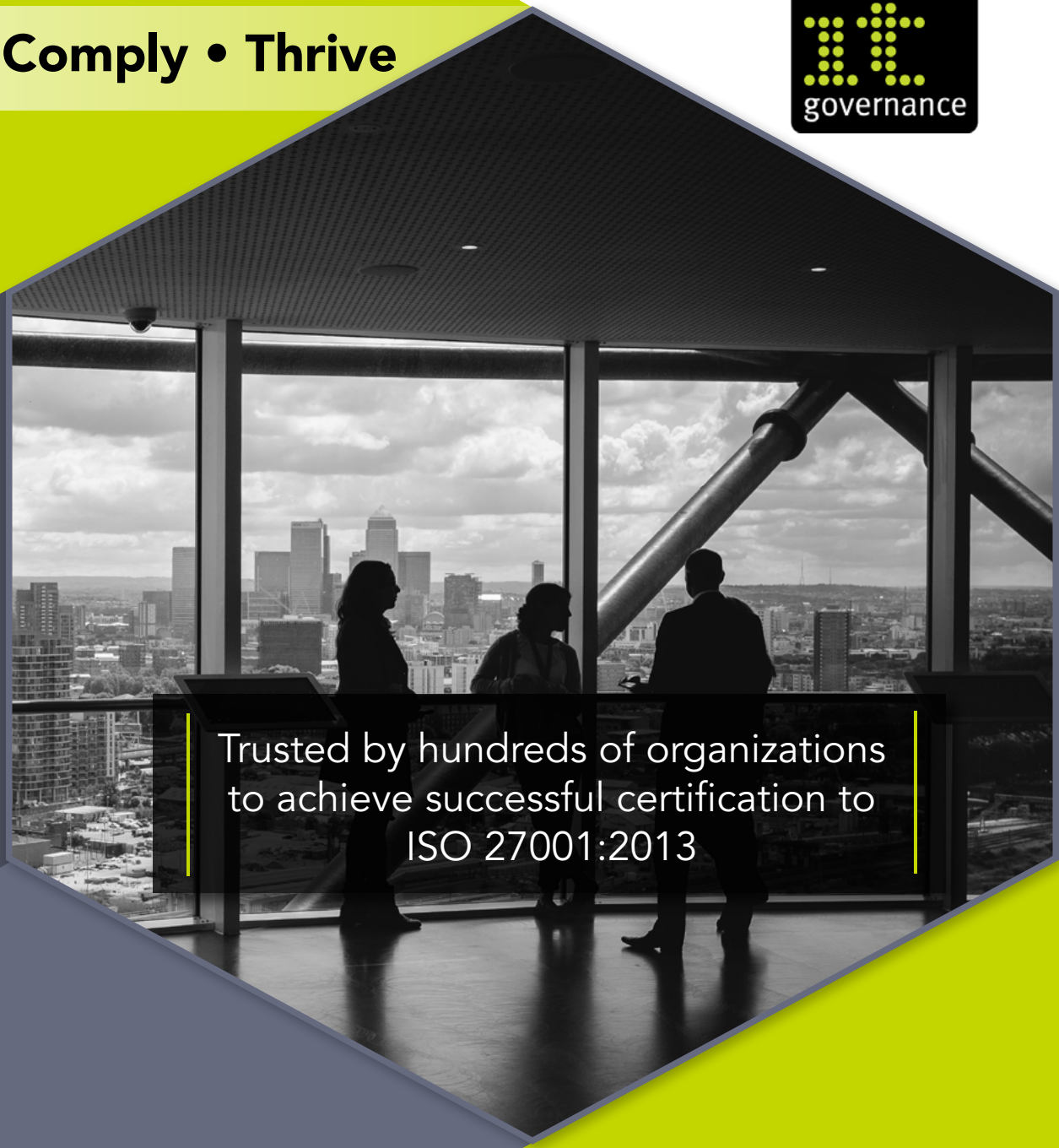
Protect • Comply • Thrive



Trusted by hundreds of organizations to achieve successful certification to ISO 27001:2013

ISO 27001 information security management consultancy

www.itgovernanceusa.com

Get a head start over your competitors and secure your critical information assets today.

Safeguard your information, your reputation and your business from the damaging effects of a data breach.

IT Governance is the world's leader in implementing information security management systems (ISMSs) that conform to the international information security standard, ISO/IEC 27001:2013. Our team led the world's first certification of an ISO 27001-compliant ISMS (information security management system).

Using a proven and pragmatic approach, we provide a variety of implementation solutions to help our clients achieve accredited certification to ISO 27001 at an agreeable cost and with minimal disruption to business.

We can show you how to get started on your project and keep it on track to achieve clear value for money from better information security management.

The IT Governance ISMS implementation approach

We have developed and honed a nine-step approach to implementing an ISO 27001-compliant ISMS. All consultancy projects led by IT Governance follow this approach, as do our training courses, guides and other tools.

A qualified consultant will work with you to ensure all the key activities of setting up a working ISO 27001 ISMS are undertaken appropriately. IT Governance will ensure that the project remains on track, and achieves its objectives, with appropriate oversight to maximize the value of the project's deliverables.

1. Project mandate

We will collate all information relating to your commitment to proceed with the project, reviewing both senior-level objectives in implementing an ISMS and 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 help the project and the ISMS deliver 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. These 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 organizational context, scope and leadership, and makes sure that the ISMS framework is aligned with and supports the business objectives.

5. Baseline security criteria

Most organizations already have a number of security controls in place. Making sure these existing security controls meet the requirements of the relevant legislation, regulations and contracts early in the project can provide significant 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 management 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. We will provide a thorough risk assessment, a Statement of Applicability (SoA) and a risk treatment plan (RTP).

7. Implementation

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

"Here we are, just 6 months after we started the project and the outcome has been described by the auditor as 'a delight to audit'. Much of this has been down to the mentoring and coaching style IT Governance has used to steer us to our goal."

David Gilbert, Global Business Development Manager, Goal Group of Companies

8. Measure, monitor and review

This stage 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 organization for the certification process. Following this, we will provide support throughout the certification audit to help with any unexpected issues that might arise.

Pre-project: ISO 27001 gap analysis

An ISO 27001 gap analysis is often the recommended place to start an ISO 27001 compliance project. Our expert-led gap analysis includes interviews with key staff and a review of your existing information security plans and documentation. The output is a detailed report that provides crucial information on:

- Your compliance gaps against ISO 27001;
- The proposed scope of your ISMS;
- Your internal resource requirements; and
- A potential timeline to achieve certification readiness.

Post-certification activities

Following certification, we can help create a plan for the maintenance and continual improvement of the ISMS.

ISO 27001 Internal Audit

Outsource your internal audit to a qualified auditor with deep experience of ISO 27001 and the audit process, and gain the assurance you need to make sure you meet your clients' and stakeholders' demands. This service consists of two separate audit days spread over one year.

ISO 27001 FastTrack™ consultancy

A fixed-price online consultancy package designed to help small organisations with 19 employees or fewer reach ISO 27001 certification readiness in just three months. Receive a 100% guarantee of certification.

ISO 27001 Managed Service

Outsource the management and maintenance of your ISMS to experts. Benefit from the reliable advice and practical experience of an ISMS specialist to manage, maintain, audit and continually improve your ISMS in line with the requirements of ISO 27001:2013.

Do-it-yourself packages

For organizations that have the resources available to get involved in an ISMS implementation project, we offer affordable DIY packages that combine bestselling tools, software, guides and qualification-based training with online consultancy.

The following DIY packages are available:

Do It Yourself:

- The core ISO 27001 standards
- 2 essential implementation guides
- vsRisk™ risk assessment software
- ISO 27001 Documentation Toolkit

Get A Little Help:

- Everything from the DIY package, plus:
- Certified Lead Implementer training course
- Certified Lead Auditor training course
- 2 hours of live, online consultancy

Get A Lot Of Help:

- Everything from the Get A Little Help package, plus:*
- Five days of structured, live, online consultancy

*excludes 2 hours of consultancy support

To find out more, visit:

www.itgovernanceusa.com/iso27001_consultancy

Why IT Governance?

100% certification guarantee

IT Governance offers a guarantee that our clients will successfully achieve certification within the timeline of the agreed ISO 27001 project. This guarantee is subject to contract and applies where the client meets the resource, competence and task completion requirements of the agreed project plan, and where the scope of the ISMS is not materially changed without agreement on both sides.

Knowledge transfer to support client independence

Where appropriate, IT Governance focuses on developing clients' knowledge and confidence in implementing and independently maintaining an effective ISMS. This approach reduces the need for continued support and minimizes any additional costs being incurred.

Demonstrable track record

IT Governance has experience of many successful management system certification and cultural change projects, with in excess of 400 consultancy clients successfully certified to ISO 27001 alone. Our ISO/IEC 27001 consultancy services use methodologies and tools that have been developed and honed over more than 15 years, beginning when two of our directors led the world's first successful certification to BS7799, the forerunner of ISO 27001.

Deep technical expertise

Our extensive expertise in ISO 27001, IT governance, the PCI DSS, ISO 22301, ISO 9001 and other leading standards means that we can help you cost-effectively integrate your ISMS with other security frameworks. Our comprehensive security solutions include Qualified Security Assessor (QSA) services for the PCI DSS and CREST-accredited penetration tests. Clients can rest assured that work is delivered by qualified and knowledgeable individuals, and meets rigorous industry standards.

Recognized by third-party accredited certification bodies

IT Governance is independent of vendors and certification bodies, and encourages clients to select the best fit for their needs and objectives. IT Governance is widely recognised amongst UKAS-accredited certification bodies as a leading consultancy and is listed on the following:

We, of course, practice what we preach:

IT Governance Ltd
Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA, United Kingdom

t: 1 877 317 3454
e: servicecenter@itgovernanceusa.com
w: www.itgovernanceusa.com

@ITGovernance /it-governance /ITGovernanceLtd