Grant Thornton
An instinct for growth™

Information Security

ISO 27001

Achieving and retaining certification

January 2018

What is ISO27001?

To give it its full title, ISO/IEC 27001:2013 is a globally recognised information security standard. It provides a flexible framework that you can apply to your business in order to build an Information Security Management System, or ISMS.

ISO 27001 is primarily a risk management tool. Information security risk assessment and treatment are core to the standard, and the controls you will implement in your organisation – policies, procedures, asset and risk registers – will enable you to mitigate the information security risks you identify.

What do I need to achieve ISO 27001 compliance?

Commitment of senior management is the core requirement for ISO 27001. Aside from approving the time and budget required for the mechanics of implementing the ISMS, senior management must ensure – by providing resources and prioritising staff time appropriately – that the controls produced by the implementation process are embedded in the normal operation of the organisation.

You will then need to define the scope of your ISMS, carry out the necessary risk assessments, and construct and implement the set of controls that will allow you to operate effectively and securely.

The members of staff within the scope of the ISMS will also need to spend time reading and understanding the various documents that make up the ISMS, and to use them on a day-to-day basis.

Finally, you must implement a regime of continual improvement: information security risks do not stand still, so an ongoing regime of reassessment and improvement is vital to remaining compliant.

One step at a time

When implementing ISO 27001 for the first time, you don't necessarily have to cover the entire organisation in a single sweep. Although you can do so if you wish, you could equally choose to begin with a modest scope (core shared services such as IT, HR and/or Finance, for instance) and then build on this in one or more further stages.

How we can help you

Grant Thornton's ISO 27001 specialists will work with you to:

- Understand how ISO 27001 can benefit your organisation.
- Define the scope and plan the implementation – in several stages if necessary – of your ISMS.
- Carry out risk assessments.
- Produce and implement the controls that will form your ISMS.
- Provide gap analyses and pre-audit evaluations to measure your level of conformity prior to formal audit.
- Educate your staff to ensure they are able to work efficiently within the ISMS.
- Arrange and oversee the formal external audit process.
- Define and implement a regime of continual improvement.

Internal expertise

Any organisation implementing ISO 27001 should look to train some key internal staff so they are able to operate of the ISMS once it is in day-to-day use. You can then focus any external support on exceptional items – expanding your ISMS scope, advising on policy breaches, and so on.

For more information please contact:

David Cartwright
Senior Consultant, Information Security
T +44 (0) 1534 885813
E david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

grantthorntonci.com