Northdown Systems
The Business Compliance Experts

What is ISO27001?

1. Introduction

In our modern world of digital transformation, on-line services and increasing cyber threats, you may have been asked whether your organisation's information security activities have been subject to independent validation – most commonly against the ISO27001 standard. To give it its full name, "ISO/IEC27001:2013" is an international standard used throughout the world, and it has become an essential requirement within many specifications and contracts. So, what's involved?

2. The ISO27001 Standard

Like all standards, ISO27001 is a published document communicating an accepted way of doing something – in this particular case securing and protecting information or data. It requires the design, implementation, operation and improvement of an ISMS – an "Information Security Management System" which is strongly focused on the identification and management of risks – both to your data and the associated IT infrastructure which processes or stores it.

More specifically, ISO27001 (using its Annex A) provides a comprehensive list of physical, technical and administrative controls – 114 in total – which are best practice activities to help protect your organisation and its data from risks.

3. Organisation Commitment

ISO27001 understands that implementing an ISMS is not a trivial activity and will require the demonstrable commitment of your Senior Management to ensure that it can become a reality. They will be responsible for defining the scope, dependencies and objectives of the ISMS, and their involvement extends to the provision of the required personnel and resources. They have an ongoing commitment too – including at formal management review sessions and in assessing internal audit reports and submitted security-related KPIs and performance data.

4. Risk Management

Risk management is at the heart of ISO27001, and whilst the standard does not define how you should undertake this task, it is clear what its outcomes should be. It will be necessary to identify and record your organisation's assets (data, premises, hardware, software etc) and for each understand that threats and vulnerabilities that could affect your data assets as a result of:

- a breach of confidentiality,
- a failure of integrity or
- a reduction in the availability of your organisation's data assets.

An assessment of the likelihood of each risk actually happening – and the impact on your organisation if it were to do so – will provide a measurement which indicates whether the risk is acceptable or not. If not, various options are available for treating the risk so that it subsequently becomes acceptable.

5. Anything Else?

The ISMS will require you to provide a comprehensive framework of readily accessible security policies and related procedures, such that your personnel, contractors, third parties etc have a clear understanding of how to undertake their activities and protect your data and assets. There is a need to provide a programme of training and awareness to assist with this objective, and records should be retained as evidence that the training has taken place.

ISO27001 also requires an understanding of the security needs and expectation of “interested parties” (e.g. your customers, stakeholders, regulators) and the assessment of security within your organisation’s supply chain (e.g. for any outsourced services, cloud-based software etc).

Like all management standards, ISO27001 mandates a programme of internal audits, such that your organisation can formally assess its performance against declared information security requirements and objectives using experienced auditors not connected with the activity being assessed.

To help measure and improve the ISMS, ISO27001 requires that a set of information security goals or objectives are established, and that your organisation takes opportunities to measure and assess its progress towards them. This further underpins another common requirement of management standards – continual improvement – which requires you to continually improve your information security posture by improving working practices, implementing more secure technology and addressing newly identified risks.

6. The Certification Process

Most organisations who implement an ISMS are focused on achieving external certification against the ISO27001 standard. This involves the selection and engagement of an external assessment body, who will arrange to visit your organisation to conduct their formal assessment in two (or three) stages.

Optionally, you may choose to ask your assessment body to undertake a gap analysis activity ahead of the formal certification activities (although if prepared well enough, this will not be required).

Stage 1 assessment is focused on the management elements, documentation and records required by the ISO27001 standard. If Stage 1 is completed successfully, the Stage 2 assessment will follow-on approximately six weeks later, which includes reviews of individual controls as well as examining how information security practices have been implemented into your organisation’s operational activities.

Successful completion of Stage 2 will allow your organisation to become ISO27001-certified and receive a certificate to that effect, typically valid for three years. However, the assessment body will need to undertake surveillance assessments every six months, to ensure that the requirements of the standard are continuing to be effectively delivered on an ongoing basis.

7. Looking for Assistance?

Northdown Systems has assisted many organisations to implement effective Information Security Management Systems and successfully achieve (and retain) formal ISO27001 certification. Our services can be customised to suit individual requirements: from an end-to-end project framework, to the provision of specialist support with risk management or the conduct of internal audits.

For more information, please visit www.northdownsystems.co.uk.