ISO/IEC 27001 : 2013

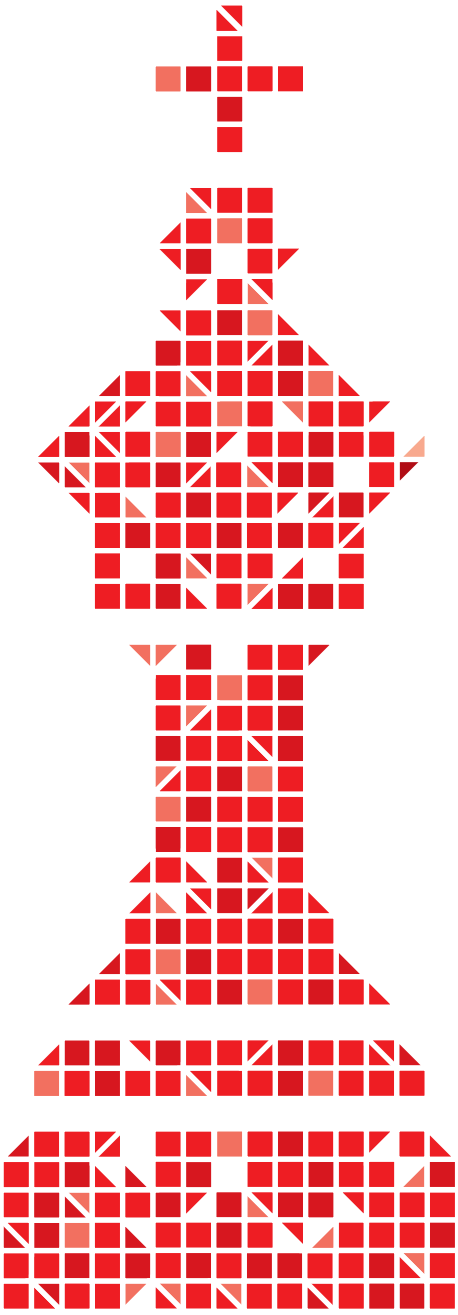
What the new approach means in practice

Red Island

Thought Leadership Paper - November 2013

v1.0

Contents



BACKGROUND

The ISO/IEC 27001 standard, originally known as BS7799, was initially developed in the 1990s by the former Department for Trade & Industry in conjunction with major companies including HSBC, Shell and Unilever.

It aimed to provide an internationally recognised code of best practice to benchmark information security management.

The basic objective of ISO/IEC 27001 is to help establish and maintain an effective Information Security Management System (ISMS), with the framework of the standard designed to fit organisations of all sizes.

It is intended to help organisations achieve a variety of different aims including ensuring that security risks are cost effectively managed, compliance with laws and regulations and providing relevant information about information security to customers.

It is independently audited, verified and certified by United Kingdom Accreditation Service (UKAS) audit bodies.

WHAT ARE THE BENEFITS OF ISO/IEC 27001?

The process of working towards ISO/IEC 27001 helps organisations understand and manage information risks in a business context.

As well as protecting the business from loss or breach of information it helps organisations take clear, informed and cost effective decisions on security controls and risk mitigation.

Perhaps most importantly it provides competitive advantage in an increasingly crowded marketplace.

Many public and private sector tenders now demand suppliers hold ISO/IEC 27001.

The UK Government is currently aiming for 50% of all new IT spend to be placed with SMEs through the Public Service Network (PSN) - effectively a secure private internet for the public sector. Compliance with many aspects of the PSN is based on the principles of ISO/IEC 27001.

With the public sector spending £7bn on IT and £1.6bn on telecoms each year, the new business opportunities through the PSN could be very significant for those who have achieved accreditation.

WHY ISO/IEC 27001 IS CHANGING

The pace of change in IT and security has meant the information security landscape has changed considerably since the standard was first introduced.

The emergence and growth of cyber crime and cloud computing together with the advent of smartphones have brought fresh challenges for organisations. Many organisations also now rely on third parties to provide at least some of their IT provision.

The revised standard aims to reflect these changes and also the experiences to date of the many organisations who have already gone down the path of certification.

The new edition of the standard seeks to provide a more flexible and streamlined approach to promote more effective risk management.

There have also been modifications to ensure the standard uses the same high-level structure as all management system standards to make integration with other ISO systems - such as the ISO 22301 standard for business continuity management - easier for organisations.

The adoption of a similar structure across standards is intended to help those looking to implement more than one management system save time and money.

WHAT THE REVISION MEANS FOR EXISTING STANDARD HOLDERS

Organisations certified to the 2005 edition of the standard will need to upgrade their ISMS to comply with the requirements of the new edition.

The transition period for upgrading is expected to be 18 months from when the new edition was published in October 2013.

At the end of this transition period, only those certificates which comply with the new requirements will be valid.

HOW IS THE APPROACH CHANGING UNDER ISO/IEC 27001?

The changes under the new standard represent a significant shift in approach.

Currently, the standard has been underpinned by the Plan-Do-Check-Act Deming cycle. Organisations would look at their existing information security provision and identify issues and gaps. They would then implement policies to deal with them, check them through internal audit and act if the policies were not proving effective.

The new approach is less prescriptive and provides organisations with more scope to interpret the guidelines, with the aim of helping them identify what they want to achieve rather than simply following a set process.

For those organisations which take a proactive approach to information security and who have a good understanding of their objectives and risks, the change in emphasis should provide more freedom.

However, greater flexibility is counterbalanced by an increased requirement from a risk treatment perspective. Organisations will have more freedom in terms of setting risks and identifying a narrow area of focus but they will have to have an effective rolling treatment plan in place.

The new standard also places more emphasis on measuring and evaluating how well an organisation's ISMS is performing.

Risk treatment moves to the fore

A greater focus on risk treatment will mean organisations and consultants may have to re-examine how they approach risk assessment.

One of the most significant changes under the new version of ISO/IEC 27001 is around the identification and implementation of controls.

Organisations will have to identify and select controls from other sources before referring to those under Annex X which will now serve as a cross-check to address any gaps.

The revision also sees risk owners rather than asset owners approve the Risk Treatment Plan – which has now become a formalised requirement - and residual risk.

These is also more focus on the standard within the wider context of an organisation and a requirement to document internal and external issues. These could include areas such as management commitment, staff motivation and shortages, lack of resources and competency, single source suppliers and market instability.

A requirement to document the needs and expectations of interested parties including legal, regulatory and contractual obligations includes external parties such as industry regulators.

Expanded scope requirements also include interested parties such as stakeholders, customers, suppliers and regulators, and businesses will now need to identify requirements in contracts, purchase orders, specifications, legislation and regulation.

The objectives of an ISMS must be more precise and fully documented with responsibilities and resource requirements and there is more emphasis on communication, both internal and external.

All important issues relevant to the ISMS including market assurance and governance goals must be documented.

The changes mean the use of audit tools to identify when specific steps have to be checked will become much less relevant under the new approach to the standard.

RED ISLAND AND ISO/IEC 27001

Red Island has taken more organisations through to ISO/IEC 27001 compliance and certification than any other consultancy.

That has given us an in-depth understanding of the problems and hurdles organisations face on the path to certification and how they can be resolved effectively and with least cost. A risk assessment tool we have developed helps clients quickly get to grips with the issues and to focus on priorities.

We look to add value throughout the process rather than just offer tick-box auditing. Our approach to ISO/IEC 27001, which has helped so many clients quickly get certification-ready is now becoming the accepted route, as the standard evolves to meet a changing world.

Risk is our business

Red Island's risk credentials are reinforced through our expertise in the Payment Card Industry Data Security Standard (PCI DSS) market where we have always focused on understanding the particular needs of a business and on risk reduction.

That experience has proved invaluable in our work with companies to help them achieve ISO/IEC 27000.

RED ISLAND & CERTIFICATION EUROPE

Red Island recently began working in partnership with Certification Europe who are primarily an ISO/IEC 27001 certification body.

We believe their value-add approach to auditing is an ideal fit for Red Island clients.

Auditing should be much more than a box-ticking exercise which can lead to a false sense of security and loss of competitive advantage. Highlighting potential issues in a constructive way is important for organisations looking to continually improve and we believe Certification Europe's approach is highly relevant to the revised ISO/IEC 27001 standard.

Red Island has a wealth of experience, a proven track record of assisting organisations with their ISO/IEC 27001 requirments and is unique in our approach with our background in Information Security Management Systems.

To find our more about how we can help you, please contact us on:

T: +44 (0) 20 7090 1091
E: info@redisland.co.uk
W: www.redisland.co.uk

London Office:
10 Fenchurch Street
London
EC3M 3BE

Company Reg. No: 4419878

Red Island