What is the ISO 27000 series of standards?

Luke Irwin 10th October 2019

The ISO/IEC 270001 family of standards, also known as the ISO 27000 series, is a series of best practices to help organisations improve their information security.

Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement an ISMS (information security management system).

An ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology.

The series consists of 46 individual standards, including ISO 27000, which provides an introduction to the family as well as clarifying key terms and definitions.

You don't need to know every standard inside out to understand how the series works, and some won't be relevant to your organisation, but there are a few core ones that you should be familiar with.

ISO 27001

This is the central standard in the ISO 27000 series, containing the implementation requirements for an ISMS. This is important to remember, as ISO 27001 is the only standard in the series that organisations can be audited and certified against.

That's because it contains an overview of everything you must do to achieve compliance, which is expanded upon in each of the following standards.

ISO 27002

This is a supplementary standard that discusses the information security controls that organisations might choose to implement.

Organisations are only required to adopt controls that they deem relevant – something that will become apparent during a risk assessment.

The controls are outlined in Annex A of ISO 27001, but whereas this is essentially a quick rundown, ISO 27002 contains a more comprehensive overview, explaining how each control works, what its objective is and how you can implement it.

ISO 27017 and ISO 27018

These standards were introduced in 2015, explaining how organisations should protect sensitive information in the Cloud. This has become especially important recently as organisations migrate much of their sensitive information on to online servers.

ISO 27017 is a code of practice, providing extra information about how to apply the Annex A controls to information stored in the Cloud.

Under ISO 27001, you have the choice to treat these as a separate set of controls. So, you'd pick a set of controls from Annex A for your 'normal' data and a set of controls from ISO 27017 for data in the Cloud.

ISO 27018 works in essentially the same way but with extra consideration for personal data.

ISO 27701

This is the newest standard in the ISO 27000 series, covering what organisations must do when implementing a PIMS (privacy information management system).

It was created in response to the GDPR (General Data Protection Regulation), which instructs organisations to adopt "appropriate technical and organisational measures" to protect personal data but doesn't state how they should do that.

ISO 27701 fills that gap, essentially bolting privacy processing controls onto ISO 27001.

Why use an ISO 27000-series standard?

Information security breaches are one of the biggest risks that organisations face. Sensitive data is used across all areas of businesses these days, increasing its value for legitimate and illegitimate use.

Countless incidents occur every month, whether it's cyber criminals hacking into a database or employees losing or misappropriating information. Wherever the data goes, the financial and reputational damage caused by a breach can be devastating.

That's why organisations are increasingly investing heavily in their defences, using ISO 27001 as a guideline for effective security.

ISO 27001 can be applied to organisations of any size and in any sector, and the framework's broadness means its implementation will always be appropriate to the size of the business.

You can find out how to get started with the Standard by reading Information Security & ISO 27001: An introduction.

This free green paper explains:

- What ISO 27001 is, how an ISMS works and how it relates to ISO 27002;
- The importance of risk assessments and risk treatment plans;
- How the Standard helps you meet your legal and regulatory obligations; and
- How to begin your ISMS implementation process.

Download now >>

About The Author

Luke Irwin

Luke Irwin is a writer for IT Governance. He has a master's degree in Critical Theory and Cultural Studies, specialising in aesthetics and technology, and is a one-time winner of a kilogram of jelly beans.

One Response

Qdot International 11TH OCTOBER 2019
nice work, keep up the good work.

SOCIAL MEDIA

Search the site

Search

CATEGORIES

- Cyber Security
  - Business Continuity
  - Cyber Essentials
  - Cyber Resilience
  - ISO 27001
  - IT Governance
    - COBIT
    - Energy Management
    - IG Toolkit
    - ISO 9001
  - NIS Regulations
  - PCI DSS