ISO 27001 is divided into 11 Sections and Annex A

INTRODUCTION

Section 0 – Is an introduction, a general overview of how ISO 27001 fits into the ISO family.

Section 1 – Provides the scope of the standard.

Section 2 – Provides the normative terms.

Section 3 – Terms and Definitions used.

PLAN

Section 4 – Context of the Organisation. Internal Issues – Business, Regulatory issues, ambitions, stakeholders include owners, employees, partners, suppliers, customers and other external bodies.

Section 5 – Leadership, management responsibilities and governance.

Section 6 – Risk Assessment, Statement of Applicability and Risk Treatment Plan.

Section 7 – Support requirements, availability of personnel, expertise, other resources, control of documentation.

DO

Section 8 – Operations, Implementation of Controls, Technical, Procedural, Personal and Physical.

CHECK

Section 9 - Perform Monitoring and Measurement, Evaluate Performance of ISMS. In effect this requires an Internal Audit, the Audit Findings (Observations and Non-conformities) Report and Management review.

ACT

Section 10 – Improvement, Corrective Action – Make the ISMS better (better, more efficient controls, added resources, smoother procedures, greater staff involvement, awareness etc.

Annex A – 114 Controls in 14 Control Sections (BUT see ISO 27002 for detail and implementation)

A.5 Information security policies – controls on how the policies are written and reviewed

A.6 Organization of information security – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking

A.7 Human resources security – controls prior to employment, during, and after the employment

A.8 Asset management – controls related to inventory of assets and acceptable use, also for information classification and media handling

A.9 Access control – controls for Access control policy, user access management, system and application access control, and user responsibilities

A.10 Cryptography – controls related to encryption and key management

A.11 Physical and environmental security – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.

A.12 Operational security – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.

A.13 Communications security – controls related to network security, segregation, network services, transfer of information, messaging, etc.

A.14 System acquisition, development and maintenance – controls defining security requirements and security in development and support processes

A.15 Supplier relationships – controls on what to include in agreements, and how to monitor the suppliers

A.16 Information security incident management – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

A.17 Information security aspects of business continuity management – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

A.18 Compliance – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

One of the biggest myths about ISO 27001 is that it is focused on IT – as you can see from the above sections, this is not quite true: while IT is certainly important, IT alone cannot protect information. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

The best way to understand Annex A is to think of it as a catalogue of security controls you can select from – out of the 114 controls that are listed in Annex A, you can choose the ones that are applicable to your company.

Relationship to the main part of ISO 27001

So, not all of these 114 controls are mandatory – a company can choose for itself which controls it finds applicable and then it must implement them (in most cases, at least 90% of the controls are applicable); the rest are declared to be non-applicable. For example, controlA.14.2.7 Outsourced

development can be marked as non-applicable if a company does not outsource the development of software. The main criterion for selecting the controls is through risk management, which is defined in clauses 6 and 8 of the main part of ISO 27001. Learn more here: ISO 27001 risk assessment & treatment – 6 basic steps.

Further, clause 5 of the main part of ISO 27001 requires you to define responsibilities for managing those controls, and clause 9 requires you to measure if the controls have fulfilled their purpose. Finally, clause 10 requires you to fix anything that is wrong with those controls, and to make sure that you achieve information security objectives with those controls.

Relationship to ISO 27002

The truth is that Annex A of ISO 27001 does not give too much detail about each control. There is usually one sentence for each control, which gives you an idea on what you need to achieve, but not how to do it. This is the purpose of ISO 27002 – it has exactly the same structure as ISO 27001 Annex A: each control from Annex A exists in ISO 27002, together with a more detailed explanation on how to implement it. But don't fall into the trap of using only ISO 27002 for managing your information security – it does not give you any clues as to how to select which controls to implement, how to measure them, how to assign responsibilities, etc. Learn more here: ISO 27001 vs. ISO 27002.

Usability of Annex A

There are a couple of things I like about Annex A – it gives you a perfect overview of which controls you can apply so that you don't forget some that would be important, and it gives you the flexibility to choose only the ones you find applicable to your business so that you don't have to waste resources on the ones that are not relevant to you.

It is true that the Annex A doesn't give you too much detail on implementation, but this is where ISO 27002 comes in; it is also true that some companies might abuse the flexibility of ISO 27001 and aim only for the minimum controls in order to pass the certification, but this is a topic for a different blog post.