ISO 27001 Introduction

Presented by: John Cato

Sources and Attributes: ISO 27001 Standard, Advisera, ISO27001Security (Gary Hinson)

Contents

- Structure
- Context of Clauses
- Mandatory Requirement Clauses
- PDCA (Plan, Do, Check, Act) Cycle
- ISO 27001:2013 Clauses and PDCA Figure
- Q & A

Structure

- The international standard for an Information Security Management System (ISMS)
- Based on 2 parts:
  - Part 1: 11 Clauses
  - Part 2: Annex A provides a guideline for 114 control objectives and controls

Context of Clauses

- Clauses 0 to 3 (Introduction, Scope, Normative references, Terms and definitions) set the introduction of the ISO 27001 standard.
- Clauses 4 to 10 provide the ISO 27001 mandatory requirements that are requirements if an organisations wants to be compliant with the standard

Mandatory requirement clauses

- 4 Context of the organization
- 5 Leadership
- 6 Planning
- 7 Support
- 8 Operation
- 9 Performance evaluation
- 10 Improvement

PDCA (Plan, Do, Check, Act) Cycle

The PDCA cycle aka Deming Cycle says the following in principle:

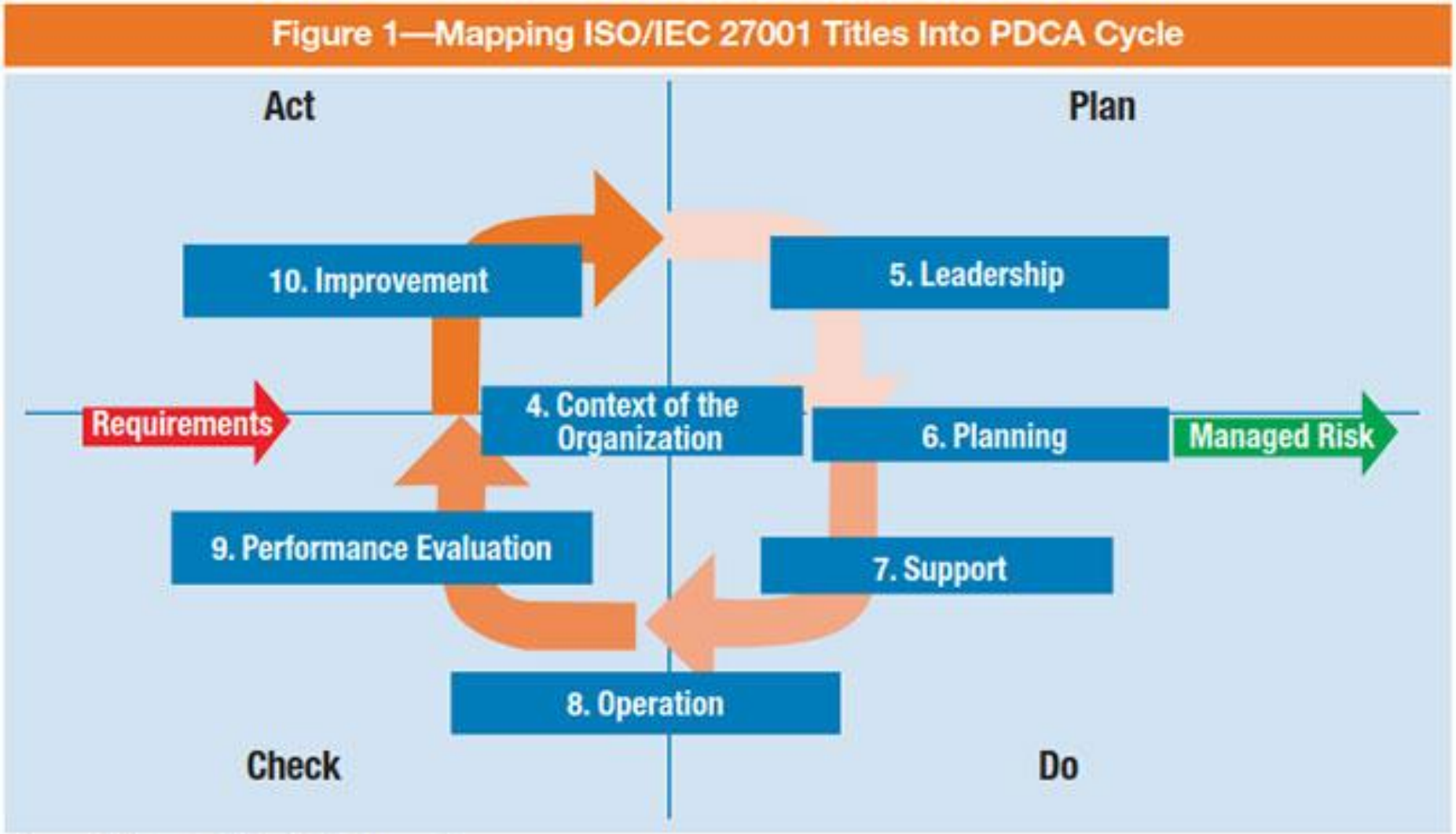
- Before you start implementing anything, you should know exactly what you really need, and exactly what it is you want to achieve (objectives) – this is the **Plan** phase.
- Once you know what you want to achieve, you can start implementing your information security, business continuity, quality procedures, or whatever the ISO standard is focused on – this is the **Do** phase.
- However, the whole effort does not stop here – you want to make sure you have achieved what you have planned for, so you need to monitor your system and measure if you achieved your objectives – this is the **Check** phase.
- Finally, if and when you realize that what you achieved is not what you have planned for, you have to fill the gap – this is called the **Act** phase

Note: This is a cyclic process which aims to enable continuous improvement and in doing so, improving the maturity level of an organisation's security posture

Has the PDCA cycle disappeared from ISO standards?

- No it hasn’t, it is still very much incorporated into ISO 27001, ISO 22301 and all other standards, only now the cycle is not expressly displayed in the introduction of the standard as was the case in older revisions.
- Here is how you can recognize the PDCA cycle in the structure of ISO standards:
  - Clauses 4 Context of the organization, 5 Leadership, 6 Planning, and 7 Support are nothing but the **Plan phase**
  - Clause 8 Operations speaks about the **Do phase**
  - Clause 9 Performance evaluation is, of course, the **Check phase**, and
  - Clause 10 Improvement is the **Act phase**

ISO 27001:2013 Clauses and PDCA Figure



Source: T. Mataracioglu. Reprinted with permission.


?
Q
&
A
!