

Proposal for the Next Version of the ISO/IEC 27001 Standard

In this article, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27001:2013 standard is introduced briefly and compared to ISO/IEC 27001:2005. The pros and cons of ISO/IEC 27001:2013 are identified by measuring against predetermined parameters. The parameters help reveal the deficiencies of ISO/IEC 27001:2013, and this article introduces a proposal for the next version of the standard.

The 2013 Version of the ISO/IEC 27001 Standard

ISO/IEC 27001 includes seven main titles described in Annex SL: organization, leadership, planning, support, operation, performance evaluation and improvement.¹ Annex SL, a high-level structure, is the outcome of work done by the ISO Technical Management Board's Joint Technical Coordination Group, and is a new management system format that helps streamline the creation of new standards and makes implementing multiple standards within one organization easier.² Using the same titles defined in Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards. Although ISO/IEC 27001:2013 does not suggest a plan-do-check-act (PDCA) cycle, the seven titles can be mapped into the cycle, as shown in **figure 1**.³

ISO/IEC 27001:2013 contains 14 control domains, shown in **figure 2**, and 114 controls.⁴

New controls added in Annex A of the 2013 version of the standard are shown in **figure 3**.⁵

Determining the Deficiencies of the ISO/IEC 27001:2013 Standard

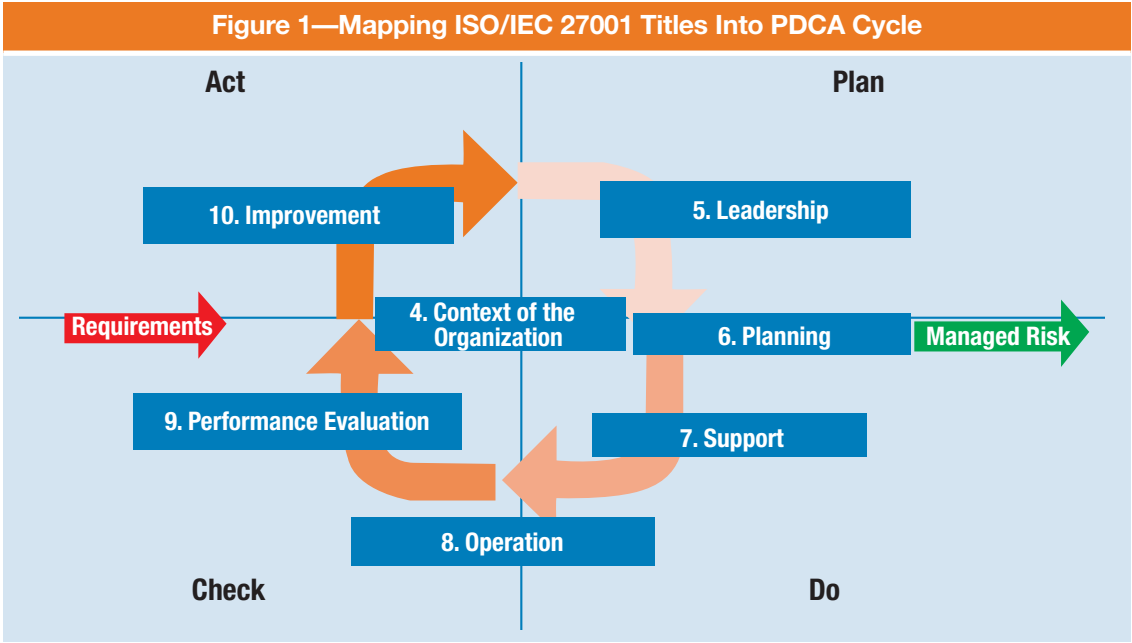
A comparison of the ISO/IEC 27001:2005 and ISO/IEC 27001:2013 standards is performed by using some predetermined parameters such as readability, understandability and applicability. Further, deficiencies of ISO/IEC 27001:2013 are determined, which will serve as an input for the proposed next version of the standard.

As explained previously, ISO/IEC 27001:2013 includes seven fixed main titles within the scope of Annex SL: organization, leadership, planning, support, operation, performance evaluation and improvement. This approach makes integration of the current system with other systems such as ISO 9001 easier, since other systems have the same fixed main titles in Annex SL. Since Annex SL does not exist in ISO/IEC 27001:2005, integration with other systems is much harder when using that version of the standard.

ISO/IEC 27001:2005 presents its clauses in chronological order, which means that information security management systems (ISMS) implementers can implement the standard from the first clause to the last one, sequentially. In contrast, ISO/IEC 27001:2013 does not use a chronological time sequence within its clauses, making ISMS implementers' jobs harder. Another parameter is applicability. Both

Tolga Mataracioglu, CISA, CISM, COBIT Foundation, BS 25999 LA, CCNA, CEH, ISO 27001 LA, MCP, MCTS, VCP

Is chief researcher and unit manager at TUBITAK BILGEM Cyber Security Institute in Turkey. He is the author of many papers about information security, published nationally and internationally. His areas of specialization are system design and security; operating systems security; governance, risk and compliance; information security management systems; business continuity; critical infrastructures; COBIT; and social engineering.



Source: T. Mataracioglu. Reprinted with permission.

Figure 2—The 14 Control Domains of ISO/IEC 27001

Control Domains	Number of Controls
A.5 Information security policies	2
A.6 Organization of information security	7
A.7 Human resources security	6
A.8 Asset management	10
A.9 Access control	14
A.10 Cryptography	2
A.11 Physical and environmental security	15
A.12 Operations security	14
A.13 Communications security	7
A.14 System acquisition, development and maintenance	13
A.15 Supplier relationships	5
A.16 Information security incident management	7
A.17 Information security aspects of business continuity management	4
A.18 Compliance	8
Total:	114

Source: T. Mataracioglu. Reprinted with permission.

Figure 3—New Controls in Annex A of ISO/IEC 27001

Control Number	Name of New Controls
A.6.1.5	Information security in project management
A.12.6.2	Restrictions on software installation
A.14.2.1	Secure development policy
A.14.2.5	Secure system engineering principles
A.14.2.6	Secure development environment
A.14.2.8	System security testing
A.15.1.1	Information security policy for supplier relationships
A.15.1.3	Information and communication technology supply chain
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to information security incidents
A.17.2.1	Availability of information processing facilities

Source: T. Mataracioglu. Reprinted with permission.

ISO/IEC 27001:2005 and ISO/IEC 27001:2013 are applicable to all types of organizations; however, implementing the 2005 version is much harder for small and medium-sized enterprises (SMEs) since the standard needs heavy documentation. An ISMS implementer has to create more than 80 documents for a generic organization when using ISO/IEC 27001:2005. On the other hand, ISO/IEC 27001:2013 is more applicable for SMEs since the documentation workload is reduced considerably. The 2013 standard empowers ISMS implementers to determine the amount and type of documentation that is appropriate to the size and complexities of the organizations.

Readability of ISO/IEC 27001:2005 is highly developed since the reader can see the plan, do, check, act (PDCA) cycle and understand the conceptual process of ISMS. Further, there is no need to jump to other standards to implement the standard's clauses. In contrast, ISO/IEC 27001:2013 does not include preliminary information such as the PDCA cycle. Also, ISMS implementers need to study other standards that are referenced in ISO/IEC 27001:2013 to implement some of its clauses.

How about the understandability of the standards? Similar to the readability parameter, it is hard to understand the requirements of ISO/IEC 27001:2013. Conversely, ISO/IEC 27001:2005 is much more understandable, even for beginners. It is quite difficult for beginner-level ISMS implementers to understand the 2013 version of the standard.

As mentioned previously, the PDCA cycle does not exist in ISO/IEC 27001:2013. Someone has to map the sections of the standard to the phases of the PDCA cycle, as shown in **figure 1**. Even then, it is not a perfect mapping since some of the clauses of the 2013 standard do not fit the same phase in the PDCA cycle. On the other hand, the 2005 standard uses the PDCA cycle, and the standard's clauses are perfectly suited to the PDCA phases.

How about performing risk analysis? Performing a risk analysis is explained step by step in ISO/IEC 27001:2005: creating an asset inventory, determining the vulnerabilities on the assets, determining the threats that use those vulnerabilities, and writing down and evaluating



the risk. This step-by-step approach may be easily understood, but it is hard to implement. In the 2013 standard, terms such as “asset,” “vulnerability” or “threat” do not exist in the main clauses. The standard does not deal with intermediary steps for writing down the risk; instead, it deals with business risk. This approach of only focusing on the business risk makes ISMS implementers' jobs easier.

“ When considering the overlapping controls, it can easily be said that there are many similar controls that mitigate the same risk in ISO/IEC 27001:2005. ”

In ISO/IEC 27001:2005, there exist 11 control domains and 133 controls. In ISO/IEC 27001:2013, there are 14 control domains and 114 controls, meaning that in the 2013 version of the standard, the number of control domains is increased even though some of the old control domains are eliminated. Thirty controls from the 2005 version are out of use in the 2013 version and 11 new controls are added.

Figure 4—Comparison and Analysis of ISO/IEC 27001:2005 and ISO/IEC 27001:2013

Parameter	ISO/IEC 27001:2005 Standard	ISO/IEC 27001:2013 Standard
Annex SL structure	Does not exist	Exists
Integration with other systems	Hard	Easy
Time sequence	Exists	Does not exist
Applicability	Hard for SMEs	Easy for SMEs
Readability	Easy	Hard
Understandability	Easy	Hard
PDCA approach	Exists	Exists indirectly
Documentation	Heavy	Depends on the size and the complexity of the organization
Risk analysis	Hard	Easy
Number of control domains	11	14
Number of controls	133	114
Overlapping controls	Significant	Occasional

Source: T. Mataracioglu. Reprinted with permission.

When considering the overlapping controls, it can easily be said that there are many similar controls that mitigate the same risk in ISO/IEC 27001:2005. On the other hand, ISO/IEC 27001:2013 is much more successful in dealing with overlapping controls.

The comparison and analysis of ISO/IEC 27001:2005 and ISO/IEC 27001:2013 are summarized in **figure 4**.

Proposal and Conclusion

This article discusses several deficiencies of the ISO/IEC 27001:2013 standard and proposes that they be considered when preparing and publishing the new version of the standard in the future. The author's suggestions for the new version of the standard, based on **figure 4**, follow:

1. The next version of the standard should list its clauses in sequential order.
2. The next version should specifically define the documentation workloads for SME's and other types of organizations.

3. The readability of the next version should be enhanced to enable easy understanding of the conceptual processes of ISMS. Further, there should be no need for frequent reference to other standards to implement the standard's clauses.
4. The new version of the standard should be understandable even for beginner-level ISMS implementers.
5. The new version of the standard should use the PDCA cycle, and the clauses of the standard should align with the phases of the PDCA cycle.
6. Although ISO/IEC 27001:2013 is much more successful than the 2005 version in addressing overlapping controls, some overlapping controls still exist. The new version of the standard should avoid all overlapping controls.

When preparing and compiling the next version of the ISO/IEC 27001 standard, the related ISO committee should take these suggestions into account so as to publish a more concrete, understandable and feasible version of the standard.

Endnotes

- 1 International Organization for Standardization, ISO Consultant Pune, "Annex SL," <http://isoconsultantpune.com/iso-90012015-understanding-structure-terminology-concept/annex-sl/>
- 2 National Organization for Standardization, ISO 22000 Resource Center, "ISO 9001:2015 DIS Version—What Is Annex SL Platform?," 23 March 2015, <http://iso22000resourcecenter.blogspot.com.tr/2015/03/iso-90012015-dis-version-what-is-annex.html>
- 3 Calik, O.; "ISO 27001:2013 Bilgi Güvenli i Yönetim Sistemi Standardındaki De i iklikler ve Yenilikler," Ulusal Bilgi Güvenli i Kapısı Hakkında, 12 May 2013, <https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html>
- 4 Richard, R.; "The New ISMS, ISO/IEC 27001:2013 Expert Insight," IT World Canada Blog, 5 September 2013, www.itworldcanada.com/blog/the-new-isms-isoiec-270012013-expert-insight/84379
- 5 BSI Group, *Mapping Between the Requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013*, <https://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf>