www.jusletter-it.eu

Daniel Ronzani

ISO 27001:2013

Category: News
Field of law: Information law
Region: Switzerland

Citation: Daniel Ronzani, ISO 27001:2013, in: Jusletter IT next: 11. September 2014 – Lachmayer

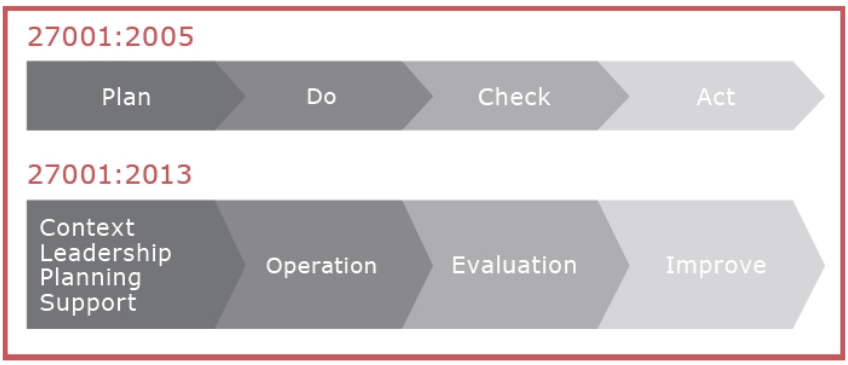
[Rz 1] ISO 27001 is a standard for an information security management system (ISMS). It helps organisations keep their assets secure[1] by establishing, implementing, maintaining and improving their ISMS.[2] This article covers some of the differences as compared to first edition of the standard (ISO 27001:2005).

[Rz 2] 1. ISO 27001:2013 has been restructured.[3] It follows the 10-section structure of the new ISO Annex SL.[4] Annex SL harmonizes structure, text, terms, and definitions.

[Rz 3] 2. Consequently, the former definition section has been removed. The terms are now standardised and referenced in the updated definitions stipulated in ISO 27000:2012.

[Rz 4] 3. The most apparent change is the omitted plan-do-check-act (PDCA) cycle of ISO 27001:2005. Hence, the new ISO structure is open for other ISMS improvement methods. The following match to the PDCA cycle crystallises the new open approach:[5]

Graph 1: Matching ISO 27001:2013 to 27001:2005.



[Rz 5] 3.1 Plan: The first element of the cycle is now distributed over four sections: Context of the organisation, where the organisation determines its issues, needs and expectations

[Rz 6] for an ISMS; Leadership, where the organisation's management demonstrates commitment to an ISMS and establishes an ISMS policy; Planning, where the organisation addresses risks and opportunities, and establishes security objectives; and Support, where the organisation shall provide resources, determine competent personnel, create awareness among the staff, and define a communication strategy.

[Rz 7] 3.2 Do: The second element of the cycle comprises the operation. The organisation plans and controls the process for the security objectives, performs risk assessments, and implements a risk treatment plan.

[Rz 8] 3.3 Check: The third element comprises the performance evaluation. The organisation evaluates the security performance and effectiveness of the ISMS, and performs an internal audit. The ISMS is reviewed regularly.

[Rz 9] 3.4 Act: The last element of the PDCA cycle now comprises the improvement. The organisa-

1 ISO, ISO 27001 ISMS, tinyurl.com/kh2t2uo.

2 Art. 1 ISO 27001:2013.

3 ISO, ISO 27001:2013 (en), tinyurl.com/lwljjqa.

4 ISO, Management Makeover, tinyurl.com/ltofr2c.

5 bsi, ISO 27001:2013, tinyurl.com/lov6ujv.

tion takes corrective actions if any non-conformity occurs, and continuously improves suitability, adequacy and effectiveness of the ISMS.

[Rz 10] 4. Annexes B (OECD principles) and C (standard correspondence) of ISO 27001:2005 have been removed. Annex A (control objectives) of ISO 27001:2013 has been restructured and revised. With qualified data protection officers[6] our law firm also provides legal support on security issues.

Daniel Ronzani

6 Art. 11a para. 5 lit. e Federal Act on Data Protection (FADP).