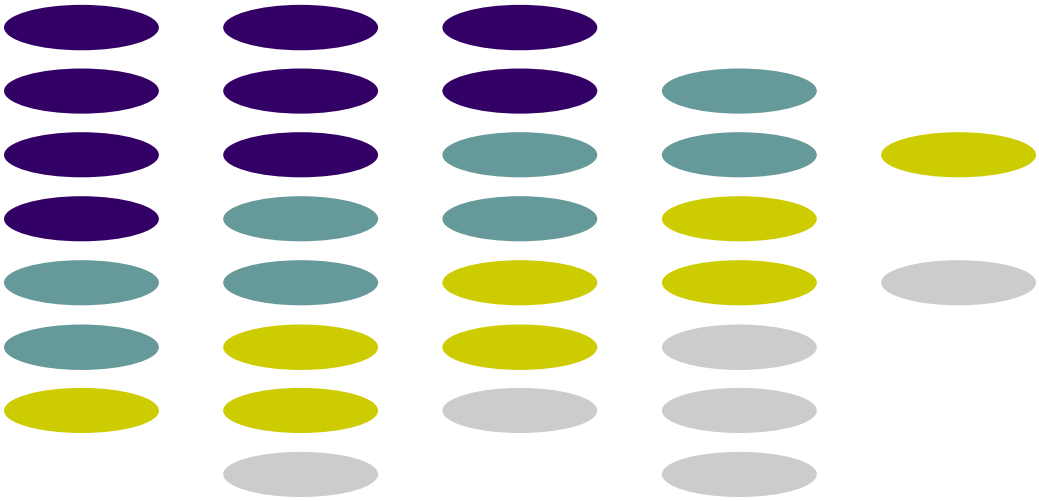
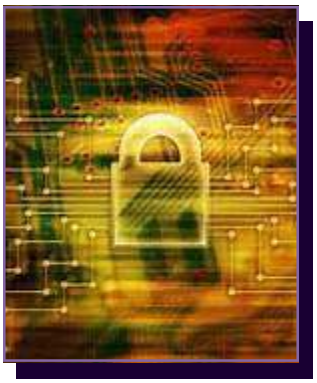


ISO/IEC 27001:2013, the simple facts

Our Mission *is to provide courteous, friendly, and ethical "adding-value-assessment" accredited registration services, as we help client-organizations meet international benchmarks with integrity, while enhancing their administrative and operating practices.*

Our Vision *is to be a consumer-centric integrated third party entity providing the most favorable option for client-organizations; not to conduct mere conformity body in justification of billing.*



ISMS ISO/IEC 27001 2013 Comparison to 2005

Year 2013 is align with other management system in the likes of ISO 22301 and being reviewed future ISO 9001 and others. The inputs from certification bodies and accreditation entities based Europe for global understandings. To this effect a new format structure arrives in ISMS ISO/IEC 27001 2013 aligning with the upcoming ISO publications as follows:

0. Introduction taking a process approach
1. Scope is not specific required thus any organization may choose to adapt without the overwhelming mandates in control
2. Normative References, in BRS we believe that these are laws and regulations an not necessarily other ISO publications
3. Terms and Definitions is a brief glossary to be superseded by ISO/IEC 27000
4. Context of the Organization, it helps in defining the scope of the ISMS, similarly to any other ISO management system, requires policies and other directives set by the organization
5. Leadership, as set by any other ISO publication
6. Planning outlines a process to identify, analyze and plan to treat information security risks, and its objectives
7. Support, combines availability of resources awareness, competence and objectiveness
8. Operation, pragmatic application to treat security risks
9. Performance Evaluation is to measure the effectiveness and seek areas to enhance operations, and
10. Improvement is through internal audit controls as the management system is the basis to enhance performance in light of changing circumstances

Interestingly there is complete relationship to the version 2005 of ISO/IEC 27001, it is just now placed within the context of 0 to 10 format structure noted above. Since this is construe as new version it open for the certification bodies to conduct special assessments or a reassessments as a new document.

Note: In ways it seems like a hybrid between was then 1994 and current 2013.

To the benefit of BRS work and client-organizations worldwide, the most significant changes are:

- The controls (Annex A) are no longer a mandate, these are set by the organization through the identification of threats, analysis and risks in order to set the appropriate controls. Surprisingly, this deletes the thought of mandating what the ISO thought is best for organizations to control. In other words, the organization is given freedom of choice thus not mandate from ISO, which is attune and practical to sovereignty of nations and enterprise in the free market.
- The Plan-Do-Check-Act is now gone. The concept of continual improvement remains.
- ISO/IEC 27002, a mandate of what to implement, is gone as it was not commercially effective to certification and accreditation bodies.
- Like ISO 9000 series there is now an ISO/IEC 27000 to provide terms and definitions across other publications within this series.
- Through 4.0 “Understanding the Organization and its Context” and “Understanding the needs and expectations of interested parties” are integral to 2013 of ISO/IEC 27001.
- The concept of the SOA is unchanged, yet deletes the mandate to select from Annex A (the controls). The inclusions and exclusions are decided by the organization and a third party assessment team review the competence of these. In BRS purpose is granted by public trust to protect the community of consumers (and not for merely conformity verification).
- Like in other risk sectors, correction and corrective action comes into play and deletes prevention element; however, BRS will continue the pursuit of identifying potential adverse issues happening elsewhere to protect client-organization, community and consumers.
- Documentation requirements is now seen under section 7.0, in ISO/IEC 27001 is 7.*5 refers to document information* in lieu of *documentation and records*.

BRS assessment teams will focus on laws and regulations (see annexes) for the purpose which we been granted accreditation with the help and through mainly the following clauses: 4.3, 5.2, 6.1.2—6.1.3, 6.2 7.2, 7.5.1, 8.1-8.3 9.1-9.3 and 10.1 and their interactivity within ISO/IEC 27001 2013. Client-organizations possess the freedom to best protect their community of consumers.

At BRS we believe that the version 2013 is a continuation of the version 2005 in a new format without the mandate to exercise specific controls, as ISO knows best. ISO/IEC 27001 2013 mandate a new review as threats and risks considering that the mandate of controls is gone. Further, we continue to seek that client-organizations adhere laws and regulations on our purpose to protect community and consumers while exercising due-care.

Contact Us Online

Reach us online

We answer requests promptly

Mission, values and vision with purpose

Find out what's happening at BRS and stay informed based on facts and not myths

BRS

31977 Hilltop Boulevard, Suite D—POB 1020

Running Springs, California USA 92382

global@brsglobal.net

www.brsltd.org — www.brsglobal.us

www.brsasiapacific.net

North America | Central America & Caribbean | South America | Euro Asia | Western Europe | Asia-Pacific | Middle East & North Africa