ISO/IEC 27001 INFORMATION SYSTEMS SECURITY MANAGEMENT STANDARD

INTODUCTION TO SECURE CODING

SEVDA CIMEN
sevdacimen23@gmail.com

Abstract

This document contains the information security technologies standards especially ISO 27001.What is all about and using areas for this standard and also this article includes the effect of developing technologies on information security.

1 History

ISO, founded on February 23, 1947, promulgates worldwide proprietary industrial and commercial standards, has headquarters in Geneva, Switzerland. [1] The international standard of ISO 27001 specifies the requirements for establishing, imple-menting, operating, monitoring, reviewing, main-taining and improving a documented ISMS within an organization

2 ISO 27001

In this century the system of software and net-work using areas getting bigger for all com-pany and users especially with cloud comput-ing,including firewall configuration, authentica-tion, and network management.For this develop-ment there is also a standard for secure our infor-mation sources.The International Organization for Standardization (ISO) has published a series of in-formation security management systems (ISMS) standards including the standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Re-quirements (ISO, 2005a). Publication of this stan-dard is intended to offer the global markets a possi-bility for harmonizing diverse IS security methods and methodologies by adopting the newly pub-lished one. In the context of the observed high interest to the topic of ISMS among practition-ers and academia, the global business informati-zation processes, and the success of ISO management system standards, one would expect to see growing attention to the standard as expressed in the number of related publications and the diffusion of ISO/IEC 27001 information security management system (ISMS) standard worldwide. [2]

3 Introduction

For the protection of the information and information systems the standards ISO 27000, ISO 27001 and ISO 27002 provide control objectives, specific controls, requirements and guidelines, with which the company can achieve ade- quate information security. [3] With a certification against ISO 27001 a company verifies the fulfillment of well-known and accepted secu- rity standards and thus pro-motes customers trust. Like- wise a verification of compliance with an international standard reduces the risk of fines or compensation pay- ments as a result of legal disputes, since legal require- ments such as provisioning according to state-of-the- art and with due care and diligence can be countered with standards compliance [3]. We present the ISO 27000 to ISO 27002 standards, their devel-opment and actual dissemination, and the ISO 27 K family of stan- dards

4 Benefits And Obstacles On ISO27001 Implementation

ISO 27001 plays a very important role in monitoring, review, maintenance and improvement of an information security management system. It works like an overall management and control framework for managing an organization's information security risks. The prime objective of this standard normally supports to establish, design, implement and manage an effective information management system which protects information

[1] ISO History and Definition. www.iso.org

[2] Weick, K. E. (1989). Theory construction as disciplined imagination. Academy of Management Review, 14(4), 516-531.

[3] Journal of Information Security, 2013, 4, 92-100

of an organization from any risks .[4] International standard ISO 27001 enables your organization to establish a security process which systematically optimizes your organizations security to a definable level. This process leads to a whole range of advantages.

4.1 List of benefits and obstacles

Proof of security to third parties (for clients, partners and legal purposes)

Competitive advantage: documented quality by an independent authority

Cost reductions through transparent, opti-mized structures.

Security becomes an integral part of business processes

Knowledge and monitoring of the IT risks and residual IT risks

Documentation of structures and processes

Increased employee awareness of security

Evaluation of the organizations processes from a security point of view.

Prioritizing the security of the business operations: business continuity management

Globally recognized standard

Potential reduction in insurance premiums

Referencing the IT process management standard (ITIL) to ISO 27001

5

5 Certification Process

To verify the compliance of the ISMS with ISO 27001 a company has to pass a certification procedure steered by an authorized certification organization (Registered Cer- tification Bodies RCB), ISO provides a list of RCBs. The company initi-ates the procedure by selecting an RCB. In a preliminary examination with the support of the RCS a determination can be made to ascertain the extent to which there already is conformity according the standard and which needs for actions still exist for successful certification.[6]

6 Analysis

Without information security, the business is faced with various negative impacts including financial consequences, weakened protection of the organizations intellectual capital and IPR, loss of mar-ket share, poor productivity and performance rat-ings, ineffective operations, inability to comply with laws and regulations, or loss of image and reputation [7]. In this section we attempt to reveal the factors for low adoption of IS security stan-dards in general, and ISO/IEC 27001 in particular. The general criticism found in literature reviewed suggests that companies in general, and SMEs in particular, are not well positioned to adopt ISMS standards [8]. However, in the tradition of system sciences [9], we believe important insights on the drivers and barriers to standards adoption can be obtained from similar past developments. A sys-temic approach to complex organizational prob-lems is to develop expectations of how the future will unfold and to define actions that would lead to more desirable predicted futures [10]. This ap-proach requires an expert knowledge from similar past developments. In this respect, we find that benchmarking the ISO/IEC 27001 standard to its well-known predecessor, ISO 9001, can inform us on future adoption of the former.

7 Conclusions

In this paper we attempted to find the reasons for little attention for ISO/IEC 27001. In doing so, we examined the adequacy of information secu-rity management system standards to the needs of organizations and attempted to reveal critical barriers for certification. Our work was motivated by the discovery that the number of publications dedicated to the ISO/IEC 27001 standard is oddly low as compared to the overall number of publications dedicated to the topic of information security management system. To make sense of the situation (Weick, 1989), we first benchmarked the ISO/IEC 27001 certification dynamics against that of two other management system standards from ISO

[4] Ali Bitazar, 2009

[5] International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[6] Journal of Information Security, 2013, 4, 92-100 Georg Disterer

[7] Humphreys, 2006, p.10

[8] Barlette Fomin, 2008)

[9] Axelrod Cohen, 1999)

[10] Axelrod Cohen, 1999

with a 20 and 10 years history ISO 14001 environmental management and ISO 9001 quality management system standards, respectively. Juxtaposition of standards diffusion rates only confirmed the initial observation, but did not elucidate the issue. Our next step was to use AbiInform (Proquest) database to analyze the publication frequencies for the three ISO management system standards. This analysis showed that ISO/IEC 27001 standard, as compared to the other two ISO standards, has received significantly less interest from academia, as measured by the number of scholarly publications on the topic. In an attempt to recon-cile the official rhetoric on the criticality of ISMS methods in general and ISO/IEC 27001 standard in particular to contemporary business operations with the observed real situation, we identified gen-eral criticism for ISMS standards. Further, in the tradition of a systemic approach to complex organizational problems (Axelrod Cohen, 1999), we compared the pros and cons of ISO/IEC 27001 to those of similar standards. Through this benchmarking, we attempted to explain the low adop-tion of ISO/IEC 27001. Given the exploratory na-ture of this research, the contribution of this work is fairly moderate [11]

8 Contribution and future research

Building on our recent literature review (Barlette Fomin, 2008), we contribute to management practice by identifying a number of important drivers for ISMS standards adoption, some of which are already in place, and some can be triggered by appropriate action. Our conclusion is that the general negative issues pertaining to ISMS should not become inhibitors to the ISO/IEC 27001 standards adoption. It appears that ISO 9001 standard has seen a steady increase of adoption over the years despite receiving virtually the same criticism as that we find for ISO/IEC 27001 standard. Given the situation with very low number of scholarly publications dedicated to ISO/IEC 27001, we call for more research on this standard. [12]

Finally, the anonymous reviewers for this paper identified several important issues for future research. One suggested reason for the low adoption of ISO/IEC 27001 in Europe and the U.S. may be related to the bias of current generation of IT specialists (CIOs, consultants, and alike, who can exert influence on the standards adoption in organizations) towards IETF standards, and not those from ISO. Another reason for the low adoption rates of ISO/IEC 27001 in post-industrial coun-tries may be related to the outsourcing of infor-mation related business to the emerging software powers in the Far East. This thesis, however, is not supported by statistics, as India, for example, by July 2008 had almost equal number of certifi-cates as the U.K. 381 and 347, respectively while Japan had 2,668 and the U.S. had only 73.5 Third issue worth investigating is the influence of busi-ness principles and norms in different countries on how company managers perceive the need for adoption vs. certification of the standard, as the statistics on the standards adoption are actually showing the numbers for certificates sold, and not the actual number of companies implementing the system management standard. [13]

[11] ISO/IEC 27001 information system security management standard:exploring the reasons for low adoption

[12] Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), 60-66.

[13] Data from ISMS user group found at http://www.iso27001certificates.com/.