Journal of Emerging Trends in Economics and Management Sciences (JETEMS) 7(6): 389-391

jetems.scholarlinkresearch.com

Analysis of management of Information security and related Enterprise risks in view of ISO/IEC 27001:2013

[1]Ashish Ukidve and [2]Milind Tadvalkar
[1]Principal, Vidyalankar Polytechnic, Mumbai, India
[2]Director, Vidyalankar Dnyanapeeth Trust, Mumbai, India

Abstract
International Organization for Standardization (ISO) and IEC- International Electrotechnical Commission formally released the updates to ISO/IEC 27001 and 27002. The last time these standards were updated was in 2005. Even though ISO/IEC 27001:2005 generally talked about monitoring the ISMS implementation, it did not clearly specify importance of having a formal documented plan or justification for monitoring specific processes and controls. The revised version of ISO/IEC 27001:2013 has set the stage for significant structural changes in the standard's individual sections with the introduction of alterations as well the number of new information security controls. Even though the text and requirements from the previous version of the standard are still there, they have been adapted to fit new and growing topics. This paper presents study and comparison of the previous and new standards and tries to identify alignment of information security with enterprise risk management using the new version of the standard. This would enable organizations in improving corporate governance and information security risk management with Enterprise Risk Management activities.

Keywords: ISMS, ISO27001:2013, corporate governance, enterprise risk, Strategic risk management

INTRODUCTION

Key Changes To The Revised Standard 27001:2013 In Comparison Of 27001:2005

The following are the key changes in the newly revised standard:

- **Introduction of ownership of risk (clauses 6.1.2 and 6.2)** —

The concept of asset owner has substituted with a new term, "risk owners," which makes management at a higher level liable and responsible for various identified risk.

By focusing on the risk-owners approach, organizations will get the flexibility to choose and implement any risk management method that better suits the organization. Also, this will in better alignment of the information security risk management activities with the activities of enterprise risk management of an organization.

- **More importance given to stakeholders (clause 4.2)—**

In the revised standard, a separate clause has been added that specifies that all interested parties must be listed together with all their requirements. This is helpful in receiving key inputs into the information security management system (ISMS) from several interested parties who will have a stake in ISMS implementation in an organization. The importance of interested parties, which can include authorities (including legal and regulatory requirements), clients, shareholders and partners, is recognized in ISO/IEC 27001:2013

- **Improved management oversight through monitoring of controls (clause 5.1)** —

ISO/IEC 27001:2005 generally talked about monitoring the ISMS implementation and the efficiency of information security controls through management oversight.

The revised standard takes a much more concentrated approach and spells out the importance of having a formal documented plan or justification for monitoring specific processes and controls through exclusive sections introduced with very solid rules. These rules explain how to set flawless objectives, who will measure them and when, and who should examine and evaluate those results. This is envisioned to bring ISMS nearer to other management processes in an organization.

- **Addressing strategic risk—**

ISO/IEC27001:2013 also comprises of upside risk (strategic risk) instead of concentrating only on downside risk (technical risk). As part of the risk management process, organizations are now required to identify opportunities and make sure these are realized. These are improved prospects of the ISMS

that will support the business, which will empower business to do things in a better way than previously.

• **Changes introduced in risk assessment (clause 6.1.2)**—

The new requirements identify risk associated with confidentiality, integrity and availability (CIA) factors rather than Assets, vulnerabilities and threats which were of prime focus. Organizations will now have the choice of deciding whether to summarize the risk they face and how to control the risk without having to first to break down vulnerabilities, asset threats and impact by individual assets. While an asset-based approach is still permitted and can achieve more rigorous protection, organizations that may have been discouraged by this load can now ease with the option provided by the revised standard. This will provide greater flexibility for organizations in choosing the way they want to assess risk to their information security. It will also provide chances for identifying strategic risk related to the information security apart from the technical risk found around IT assets.

• **Enhanced communication on information security (clause 7.4)**

In the previous version of the standard, not much stress was given to communication of information security implementation in an organization. There is a clause added in the revised standard where all the communication requirements (e.g. who should communicate, what needs to be communicated, when, through which channel etc) are summarized. This is meant to help overcome the problem of information security being regarded as only an "IT entity" or a "security thing."

• **Changes in the count of control sections and controls —**

This change has resulted in the elimination of some controls, the addition of other controls, the necessity of some new documents and the exclusion of some unnecessary documents.

The number of controls has reduced from 133 to 114, while the number of sections has improved from 11 to 14 (Table1 and Table 2). The structure of some of the sections has been changed to be suitable for better arrangement of controls for implementation.

Table -1 - Comparison of Number of Controls

	ISO 27001:2005	ISO 27001:2013
No. of Sections in Annex A	11	14
No. of Controls in Annex A	133	114

Table -2 - New Security Controls in ISO-27001:2013

New Security control section	Description
A6.1.1	Information Security in Project Management
14.2.1	Secure development policy
14.2.5	Secure system engineering principles
14.2.6	Secure development environment
14.2.8	System security testing
16.1.4	Assessment of and decision on information security events
17.2.1	Availability of information processing facilities

SYNCHRONISATION WITH OTHER GLOBAL FRAMEWORKS & STANDARDS

The revised standard is aligned with most of the global management system standards practiced in the industry (Figure 1). It is also important to note that the revised standard has a strong focus on aligning information security management with enterprise risk management (ERM) practices.

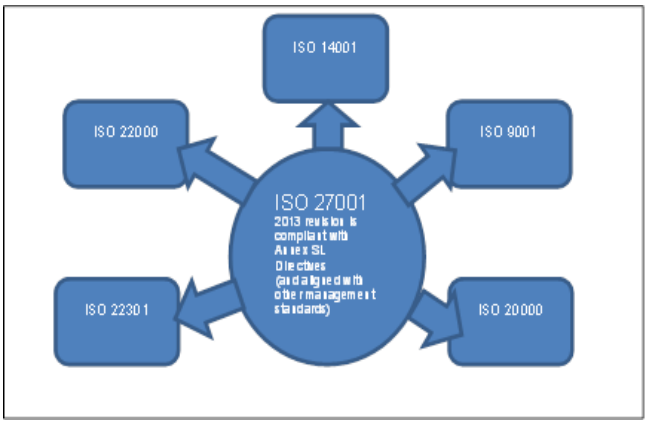

Fig – 1 - Alignment with other standards

BENEFITS FOR IMPLEMENTATION OF REVISED STANDARDS ISO/IEC 27001:2013

The updated standard can be implemented for the following purposes:

- **Improving corporate governance**—Reducing the financial exposure to the risk of losses of an organization, resulting from IT system failure is now a corporate governance requirement. ISO/IEC 27001 can help companies comply this requirement.
- **Synchronization with ERM**—The newer version aligns information security risk management (ISRM) with ERM activities.
- **Fighting cybercrime**—Introducing the ISO/IEC 27001 ISMS will help protect businesses from the threat of organized crime.

- **Recovering from accidents**—Organizations can minimize the risk that information will be lost or corrupted as a result of human error.

CONCLUSION

This paper presents study and comparison of the previous and new standards to analyze and identify alignment of information security with enterprise risk management using the new version of the standard.

ISO/IEC 27001:2013 will help organizations in aligning ISRM practices completely with the ERM practices of organizations due to flexible context-based risk assessment practices and the enhanced management oversight.

This would enable organizations in improving corporate governance and information security risk management with Enterprise Risk Management activities. However, thorough analysis of post implementation scenario of the new standard i.e 27001:2013 vis-a-vis the earlier standard needs to be done to verify confirm our findings.

REFERENCES

"Does ISO 27001Certification Make You NIST Cybersecurity Framework Compliant?" Information Security Blog, www.pivotpointsecurity.com/risky-business/iso-27001-nist-cybersecurity-framework-compliance

International Organization for Standardization (ISO), ISO 27001:2013 Information technology—Security techniques. Information security management systems— Requirements, 2013

ISACA, COBIT® Process Assessment Model (PAM):Using COBIT® 5, 2013, www.isaca.org/cobit

ISACA, COBIT 5, USA, 2012,www.isaca.org/cobit p. 13-33

ISACA, The Business Case Guide: Using Val IT 2.0, USA,2010, www.isaca.org

International Organization for Standardization(ISO)/International Electrotechnical Commission (IEC),ISO/IEC 27001:2005, Information technology—Security techniques—Information security management systems—Requirements, 2005, www.iso.org/iso/catalogue_detail?csnumber=42103