Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 194-206

Physical and Logical Security Risk Assessment Procedure for SMEs, according to ISO/IEC 27005:2011 and SR ISO 31000:2010 Standards

Marian FIROIU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
mfiroiu@hotmail.com, bacivaro@euroqual.pub.ro

Abstract
This paper proposes an assessment procedure for physical and logical risk security for small and medium-sized enterprises. This procedure relies on SR ISO 31000: 2010 and ISO/IEC 27005: 2011 standards, is created step by step as a working model and is sustained by concrete examples facilitating the understanding of the risk assessment and analysis. This procedure is meant to be a useful and an easy tool for specialists who are concerned with security risk assessment.

Keywords: organization, security, risk, standards, SR ISO 31000, ISO/IEC 27005, procedure, risk management
system, information security, risk assessment, physical security

References:

[1] *** ISACA (2007), CISM review manual, ISACA, p. 77.
[2] https://en.wikipedia.org/wiki/Security_convergence, accessed on 15th of February 2016.
[3] http://www.gie.eu/index.php/publications/cat_view/2-giepublications77, accessed on 15th of February 2016.
[4] *** ISO (2011), ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management.
[5] *** ISO (2010), SR ISO 31000:2010 - Risk management - Principles and Guidelines on Implementation.
[6] Firoiu, Marian (2015), General Considerations on Risk Management and Information System Security Assessment According to ISO/IEC 27005:2011 and ISO 31000:2009 Standard, Quality-Access to Success, Vol. 16, Nr. 149, pp. 93-97.
[7] Shortreed, John (2010), ERM Frameworks, in: Fraser, John R.S. & Simkins, Betty J. [ed.], Enterprise Risk Management, Hoboken, New Jersey: John Wiley & Sons.
[8] Michael E. Whitman and Herbert J. Mattord (2012), Principles of Information Security, Course Technology, Cengage Learning, https://www.cengagebrain.co.nz/content/whitman38214_1111 138214_02.01_chapter01.pdf,accessedon16thofFebruary 2016.
[9] Bacivarov, Ioan C., Firoiu, Marian (2008), Risk Assessment for Critical Infrastructures, Proceedings of the Conference on Quality and Dependability CCF 2008, Sinaia, Romania.
[10] *** (2013), SR BS 31100:2013 - Risk management - Code of practice and guidance for implementation SR ISO 31000.

Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 194-206
[11] *** ENISA (2006), https://www.enisa.europa.eu/.../risk-management/ .../information-package/ Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs) - ENISA ad hoc working group on risk assessment and risk management.