Mechanics Transport Communications

Academic journal http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 13, issue 3/1, 2015
article № 1158

RISK MANAGEMENT IN NIST AND ISO/IEC 27K INFORMATION SECURITY MANAGEMENT STANDARDS' FAMILY – A BRIEF ANALYSIS

Maciej Szmit[1], Anna Szmit[2]
maciej.szmit@gmail.com, agorecka @p.lodz.pl

[1]Orange Labs; Obrzeżna 7, 01-261 Warsaw,
[2]Department of Management Technical University of Lodz; Piotrkowska 266, 90-924 Lodz; POLAND

Key words: *Information security management, Risk management, ISO/IEC 27001*

Abstract: *Risk management approach (in contrast to deterministic, compliance-based strategies) is the most popular one in contemporary security management[1]. There are a lot of methodologies, frameworks and standards concerning information's and information systems' security referring to the concept of risk management. This approach is also implemented in ISO standards – beginning from ISO 31000 – especially in ISO/IEC 27k family, the most important standards family concerning information security. NIST (National Institute of Standards and Technology – a U.S. federal agency within the U.S. Department of Commerce) has developed a set of publicly available guidance documents concerning different aspects of information systems' security (also based on risk management approach) intended primarily for U.S. federal government organizations. The aim of this article is to analyze the selected NIST documents for the proposed methods and ways of risk management.*

ISO/IEC 27k STANDARDS FAMILY

ISO 27k is a standard family developed by International Organization for Standardization (ISO). The two main original standards (27001 and 27002) derived from British Standards BS PD 003:1993 and next from BS 7799-x concern ISMS (Information Security Management Systems), but the rest of the rapidly growing family is devoted to cover the wide spectrum of information security issues. The current state of ISO/IEC 27k family[2] is shown in the table below.

Table 1.

ISO/IEC standard number	ISO/IEC standard name
27000	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
27001	Information technology -- Security techniques -- Information security management systems -- Requirements

[1] See e.g.: [1], [2], [3], [4], [5] p. 65, [6] p.197.
[2] NP – new proposal; TR – technical report; CD - Committee Draft.

27002	Information technology -- Security techniques -- Code of practice for information security controls
27003	Information technology -- Security techniques -- Information security management system implementation guidance
27004	Information technology -- Security techniques -- Information security management -- Measurement
27005	Information technology -- Security techniques -- Information security risk management
27006	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
27007	Information technology -- Security techniques -- Guidelines for information security management systems auditing
TR 27008	Information technology -- Security techniques -- Guidelines for auditors on information security controls
27009 (under development)	Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 – Requirements
27010	Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications
27011	Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
-	ISO 27012 - The project to create a standard ISO / IEC 27012 Information technology - Security techniques - Information security management systems guidelines for electronic government was canceled in 2009
27013	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27014	Information technology -- Security techniques -- Governance of information security
TR 27015	Information technology -- Security techniques -- Information security management guidelines for financial services
TR 27016	Information technology -- Security techniques -- Information security management -- Organizational economics
27017 (under development)	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
27019	Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
-	ISO 27020 standard concerns dentistry
NP 27021 (under development)	Information technology -- Security techniques -- Competence requirements for information security management systems professionals
-	
TR 27023 (under development)	Information technology -- Security techniques -- Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
-	ISO 27025 standard concerns space systems
-	ISO 27026 standard concerns space systems
-	ISO 27027 standard concerns space systems
27031	Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
27032	Information technology -- Security techniques -- Guidelines for cybersecurity
27033-1	Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
27033-2	Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
27033-3	Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
27033-4	Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways
27033-5	Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

27034-1	Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts
NP 27034-3 (under development)	Information technology -- Security techniques -- Application security -- Part 3: Application security management process
27034-2 (under development)	Information technology -- Security techniques -- Application security -- Part 2: Organization normative framework
CD 27034-4 (under development)	Information technology -- Security techniques -- Application security -- Part 4: Application security validation
CD 27034-5 (under development)	Information technology -- Security techniques -- Application security -- Part 5: Protocols and application security controls data structure
NP 27034-5-1 (under development)	Information technology -- Application security -- Part 5-1: Protocols and application security controls data structure -- XML schemas
27034-6	Information technology -- Security techniques -- Application security -- Part 6: Security guidance for specific applications
NP 27034-7 (under development)	Information technology -- Application security -- Part 7: Application security assurance prediction
27035	Information technology -- Security techniques -- Information security incident management
27036-1	Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
27036-2	Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Requirements
27036-3	Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security
CD 27036-3 (under development)	Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud services
27037	Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
27038	Information technology -- Security techniques -- Specification for digital redaction
27039	Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems (IDPS)
27040	Information technology -- Security techniques -- Storage security
27041 (under development)	Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method
27042 (under development)	Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence
27043	Information technology -- Security techniques -- Incident investigation principles and processes
27044 (under development)	Guidelines for Security Information and Event Management (SIEM)
-	ISO standard 27048 standard concerns Radiation protection
CD 27050-1 (under development)	Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts
27050-2 (under development)	Information technology – Security techniques – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery
NP 27050-3 (under development)	Information technology – Security techniques – Electronic discovery – Part 3: Code of Practice for electronic discovery
NP 27050-4 (under development)	Information technology – Security techniques – Electronic discovery – Part 4: ICT readiness for electronic discovery
ISO 27789	Health informatics -- Audit trails for electronic health records
ISO 27799	Health informatics -- Information security management in health using ISO/IEC 27002

From this article's point of view the most interesting are two standards: ISO/IEC 27002, where one can find a set of 114 Information Security Controls grouped into 14 groups (including controls concerning IT security) and ISO/IEC 27005 strictly devoted to information security risk management.

NIST STANDARDS

NIST - National Institute of Standards and Technology (between 1901 and 1988 the National Bureau of Standards also known as a National Metrological Institute), is a US government agency (agency of the United States Department of Commerce) [3]. From Information security point of view a special attention should be paid to NIST Computer Security Division's publications, which are collected in four series:

- Federal Information Processing Standards (FIPS): security standards;
- NIST Special Publications (SPs): security guidelines and recommendations. There are two subseries:
  - SP 800-series (computer security) and
  - Part of SP 500-series (information technology) publications relevant to computer security;
- NIST Interagency or Internal Reports (NISTIRs): documentation that supports and provides background information for FIPS and SPs; and
- Information Technology Laboratory (ITL) Bulletins: monthly overviews of NIST's security publications, programs and projects[4].

However NIST documents are primarily addressed to US Government organizations, they play important role in information security literature. Some of NIST recommendations and guidelines may be useful for other organization, including commercial enterprises, especially after withdrawal of ISO 13335-x (called GMITS – Guidelines for the Management of Information Technology Security[5]), because of rapid grown of ISO/IEC 27k family and because of the variety of different, sometimes incompatible, security methodologies, the situation of IT security standards seems to be very dynamic, which can create some problems during building and documenting IT security systems.

There are a few NIST SP, NIST IR and NIST ITL bulletins strictly devoted to risk management, from this article point of view the most important is the Risk Management framework defined as "the process that information system managers apply to balance the operational and economic costs of protective measures for their information and information systems with the gains in capabilities and improved support of organizational mission that result from the use of efficient protection procedures" [6] introduced in [10], [11] and document [8] that includes NIST Guide for Risk Assessment.

---

[3] The standardization organization in the USA that supervise the process of development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States and coordinates U.S. standards with international standards is American National Standards Institute (ANSI), which is also member of ISO.

[4] See: [1].

[5] There were five standards in the ISO 13335 series:

- 13335-1 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
- 13335-2 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security
- TR 13335-3 Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
- TR 13335-4 Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
- TR 13335-5 Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security

It is interesting that although ISO 13335-1 is currently withdrawn, the national standards based on it are still valid (e.g. Polish Standard PN-I-13335-1:1999, see: [9]).

[6] [10] p.2.

NIST RMF FRAMEWORK

The RMF Framework[7] consists of six steps: Categorize, Select, Implement, Assess, Authorize and Monitor (see: Figure 1).

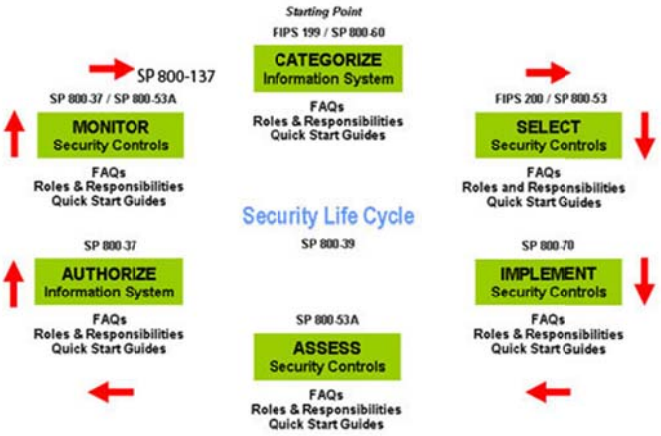

Figure 1. NIST Security Life Cycle. Source:[7].

However the RMS stands for Risk Management Framework, the lifecycle concerns no risk lifecycle but security lifecycle[8]. RMS cycle slightly differs from COBIT Risk Management Strategy cycle (see: Figure 2) or ISO/IEC 27005 Risk Management Cycle (see: Figure 3).

Figure 2. COBIT Risk Management Strategy. Source:[12].

The differences between NIST and ISO/IEC cycle are implicated – among others – by conditions relating to the law and regulation rules that must be preserved in the US government organizations. The other obvious difference between ISO/IEC approach and RMF is set of security controls. The current revision (4) of NIST SP 800-53 ([13]) includes 240 controls grouped in 18 groups. There is mapping between NIST SP 800-53 and ISO/IEC 27001 controls (and ISO 15408 requirements) in [13] (appendix H) but there are a few NIST controls that have no equivalents in ISO/IEC 27001. The NIST SP 800-53 controls are also used in NIST cybersecurity framework[9].

CONCLUSIONS

Although NIST Risk Management Framework as well as other NIST documents are obviously intended to apply in the US government organizations, what implies their limited

[7] See: [10], [11].
[8] Risk and security are obviously not the same, even in information security risk management. The risk is usually defined as effect of uncertainty on objectives and information security is defined as preservation of a set of properties such as confidentiality, integrity, availability of information and other properties. See e.g.: [2].
[9] The map of cybersecurity related controls and its equivalent in ISO/IEC 27001, COBIT and other standards may be found in [14].

applicability, it may be usefull as an aid in information security risk management in other, even commercial organizations. A big advantage of the framework is its public availability, and good readability.

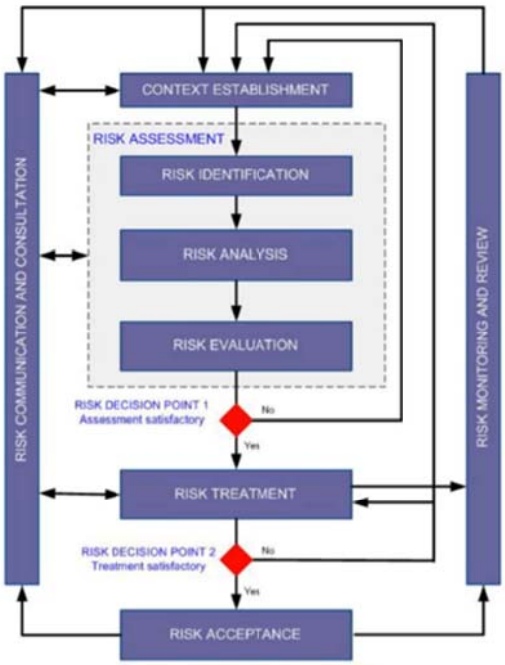

Figure 3. Risk Management Cycle in ISO 27005. Source: [7].

REFERENCES:

[1] Szmit M.: A Few Words About Technical Information Security Risk Management In IT Projects, ИНФОРМАЦИОННА СИГУРНОСТ 2014, Свищов, 2015 (INFORMACIONNA SIGURNOST 2014, Sviszov 2015)

[2] Szmit M.: Security Management And Risk Management Approach In Cybersecurity And Information Security Management, 20. Medzinárodná vedecká konferencia Riešenie krízových situácií v špecifickom prostredí, Fakulta bezpečnostného inžinierstva ŽU, Žilina, 20. - 21. máj 2015, pp. 651-656

[3] Lusková M., Buganová K.: Risk management and transport companies, Mechanics, Transport, Communications, 2011, art. ID: 491, http://www.mtc- aj.com/library/491_EN.pdf

[4] Спиридонова Х., Андонов А., Михова М.: Анализ и оценка на риска при защита на информацията в аналитични системи за управление (Spiridonova Ch., Andonov A., Michova M.: Analiz i ocenka na riska pri zaszczita nainformacijata v analiticzni sistemi za upravlienie), Mechanics, Transport, Communications, 2013, art. ID: 863

[5] Loveček T.: *Bezpečnosť* informačných systémov, Žilina 2007

[6] Korzeniowski L.F.: Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008,

[7] International Organization for Standardization homepage http://www.iso.org

[8] NIST SP 800-30, Guide for Conducting Risk Assessments (Revision 1) http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[9] Polish Standardization Committee homepage http://www.pkn.pl

[10] NIST ITL July 2009 Risk Management Framework: Helping Organizations Implement Effective Information Security Programs http://csrc.nist.gov/publications/nistbul/july2009_risk-management-framework.pdf

[11] NIST RMF overview http://csrc.nist.gov/groups/SMA/fisma/framework.html

[12] Lokuciejewski P., Wilop K., Syndikus W.: Using COBIT to Support IT Risk, COBIT

Focus vol. 4/2011, p. 15; http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Documents/COBIT-Focus-Vol-4-2011.pdf
[13] NIST 800-53 (revision 4) Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[14] NIST Cybersecurity framework http://www.nist.gov/cyberframework

КРАТЪК ПРЕГЛЕД НА УПРАВЛЕНИЕТО НА РИСКА В НАЦИОНАЛНИЯ ИНСТИТУТ ПО СТАНДАРТИЗАЦИЯ И ТЕХНОЛОГИИ НА САЩ И СТАНДАРТИТЕ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Maciej Szmit[1], Anna Szmit[2]
maciej.szmit@gmail.com, agorecka @p.lodz.pl

[1]Orange Labs; Obrzeżna 7, 01-261 Warsaw,
[2]Department of Management Technical University of Lodz; Piotrkowska 266, 90-924 Lodz; POLAND

Ключови думи: *управление на информационната сигурност, управление на риска, ISO/IEC 27001*

Резюме: *Подходът за управление на риска е един от най-популярните при съвременния мениджмънт на сигурността. Съществуват множество методи и стандарти, отнасящи се до управление на риска по отношение сигурността на информацията и информационните системи. Този подход се прилага също така и при ISO стандартите –ISO 31000 и по-конкретно групата ISO/IEC 27k, която обхваща най-важните стандарти, отнасящи се до информационната сигурност. Американският Национален Институт по Стандартизация и Технологии (НИСТ) е разработил публично достъпен наръчник по информационна сигурност за целите на правителствените институции на САЩ. Настоящият доклад има за цел да анализира подбрани документи на НИСТ, така че да бъдат представени различни методи за управление на риска.*