Information Security Management System Standards: A Gap Analysis of the Risk Management in ISO 27001 and KATAKRI

Riku Nykänen, Mikko Hakuli
University of Jyväskylä, Jyväskylä, Finland
riku.t.nykanen@student.jyu.fi
mikko.s.hakuli@student.jyu.fi

Abstract: An information security management system (ISMS) provides controls to protect organizations their most fundamental asset, information. Risk management is an essential part of any ISMS. ISO27001 is a widely adopted ISMS standard that sets specific information security requirements for the management system. Organizations that claim to have adopted ISO27001 can be formally audited and certified to comply with the ISO27001 standard. KATAKRI is a Finnish national security auditing criteria that is based on several ISMS standards and best practices. It was initially intended to be used by public sector to audit private sector service providers, but it has been adopted also as a baseline of requirements for private sector security standards. Since many organizations have claimed ISO27001 certification, it is beneficial to analyse the gaps between ISO 27001 and national KATAKRI certifications. This paper explores structures of ISO 27001 and KATAKRI and presents results of gap analysis of risk management requirements between ISO 27001 controls for information security management and KATAKRI requirements.

Keywords: information security management system (ISMS), risk management, ISO 27001, KATAKRI

1. Introduction

Risk management is an essential part of all major information security management systems. One of the key objectives of risk management is to identify and secure key assets to enable business operations and their continuity. The information technology causes a number of risks in performing operational activities and these risks are expected to continue to escalate as new technologies emerge (Pereira and Santos, 2010).

Information security helps to mitigate the various risks through the application of a suitable range of security controls (Posthumus and von Solms, 2004). Each industry operates in different risk environment. In addition to common risks each organization has its own unique risks. Hence organizations continuously struggle to choose and implement the cost efficient set of security controls that mitigates the risks to acceptable level. (Baker and Wallace, 2007)

Many organizations apply certification for their ISMS to convince their stakeholders that security of organization is properly managed and meets regulatory security requirements (Broderick, 2006). Security aware customers may require ISMS certification before business relationship is established (KATAKRI, 2011). As there is a variety of different ISMS approaches available, organizations may even be requested to have multiple certifications.

ISMS standards are not the silver bullet and they possess potential problems. Usually guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based to common, traditional practices take into consideration differences of the organizations and organization specific security requirements. (Siponen and Willison, 2009)

In this study we compare the internationally widely used ISO/IEC 27001 to Finnish national ISMS approach called KATAKRI. Comparison is limited to risk management requirements of ISMS. The paper is structured as follows: in the section 2 an overview of risk management as part of ISMS and overview of selected standards are presented. In section 3 we briefly present need for gap analysis and present a model of how the requirements were divided into phases for analysis; section 4 presents summary of the results of the gap analysis; conclusions of the results of the gap analysis are presented in section 5; discussion and future work are presented in section 6.

2. Risk management as part of information security management

2.1 Risk components in security ontology

Area of security involves people with different roles within organizations. This emphasizes the role of common understanding of the used terminology. Comprehensive study of security ontologies (Blanco et al., 2011) denotes that security community, including risk analysis community, lacks common ontology thus there exist many domain specific ontology definitions.

Risk components should be identified in Certification and Accreditation (C&A) process requiring risk management (Gandhi and Lee, 2007). ISO/IEC definitions are commonly used for terms asset, vulnerability, threat and control. Assets are something having value for the organization and what needs to be protected. Countermeasures can mitigate or reduce vulnerabilities to acceptable level. Control (countermeasure) is a mean of managing risk, including policies, procedures, guidelines, practices or organizational structures. Threat a potential cause of an unwanted incident, which may result in harm to a system or organization. Vulnerability is a weakness of an asset or group of assets that can be exploited by threats. (ISO/IEC 27002) In this paper we use previous ISO/IEC definitions unless otherwise stated.

2.2 Definition of requirements for ISMS

Desirable and “complete” security requirements cover seven facets: who, where, what, when, why, which and how? Structured requirement definitions with well-designed requirement attributes provide clearer, concise, and informative requirements compared to natural language requirement definition. (Lee et al., 2006)

C&A requirements are generally written in natural language instead of structured requirements (Gandhi and Lee, 2007). According to Lee et al. (2006) natural language requirements suffer from range of problems related to, for example, consistency, completeness and redundancy. Natural language requirements are often long and verbose, but decomposing a requirement may change the meaning or context of the requirement. However, decompositions ease requirement compliance evaluation. Another problem is varying requirement abstraction levels. Decomposition and restructuring is a solution for this problem also. The third addressed problem in the natural language requirements is that requirements suit to multiple requirement categories. The last of the presented problems is having redundant requirements. The same requirement may be expressed even within same document using different terminologies.

2.3 ISO/IEC 27000 standards family

ISO/IEC 27001 is an information security standard published by the ISO/IEC standardization organization in 2005. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. ISO/IEC 27001 specifies requirements for the management of the implementation of the security controls. The controls and implementation guidelines than an organization may use are presented in ISO/IEC 27002. Controls represented in appendix of ISO/IEC 27001 and in ISO/IEC 27002 are normative. Organization defines which of the controls it shall implement. Organization may request certification against ISO/IEC 27001 for implemented ISMS. ISO/IEC 27001 contains definition of the term and definitions. Definitions refer to other ISO/IEC standard documents. Hence all ISO/IEC 27000 family standards share a common ontology.

ISO/IEC 27001 describes four-phase cyclic process known as “Plan-Do-Act-Check” (PDCA).

- Plan: establish security policy, objectives, processes and procedures.
- Do: implement the security policy and relevant procedures.
- Check: assess and measure the process performance.
- Act: take corrective and preventive actions.

Applying PDCA model, organization adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS. ISO/IEC 27000 Information Security Management System standards family includes also ISO/IEC 27005 standard for risk management. Its purpose is equal to ISO/IEC 27002 as it provides implementation guidance that can be used when planning risk management activities.

Boehmer (2009) claims that ISMS based on ISO 27001 is equivalent to risk management, which again is equivalent cost/benefit management. Risk approach is in the interest of organizations that want to avoid wasting investments in information security, and to find cost-efficient, risk mitigating controls.

2.4 KATAKRI – Finnish national security auditing criteria

Another approach to manage corporate security is Finnish national security auditing criteria, KATAKRI. It is published by the ministry of defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority, ministry of foreign affairs and ministry of the interior have also participated in the preparation of the criteria. Initial version was published in 2009 and the updated version II in 2011.

The first goal of national security auditing criteria is to harmonize official measures while assessing organization security level. The second defined goal is “to support companies and other organizations as well as authorities with their service providers and subcontractors to work on their own internal security”. Therefore criteria contain unofficial recommendations to help users to apply useful security practices. (KATAKRI, 2011)

KATAKRI is organized as requirements compliance questionnaire. It defines a number of requirements in form of questions. Each question consists of a tripartite classification of criteria, corresponding to the security level concepts: the base level (level IV), the increased level (level III) and the high level (level II). For KATAKRI certification the organization shall select the pursued security level. Based on selection, every criterion defined for the selected security level must be complied in each question. The questions and criteria are defined in natural language.

Criteria are divided into four main areas:

- administrative security
- personnel security
- physical security
- information security

Areas are not meant to be used independently. It is instructed to take all four areas into account when performing accreditation audit using KATAKRI. (KATAKRI, 2011)

KATAKRI does not include definition of terminology that is used. Each question contains, in addition to requirements to all security levels, two columns; “recommendations for the industry” and “source/additional information”. For the questions having sources defined, definitions of terms can be derived from defined requirement sources. Lack of the common ontology can be seen as major weakness of KATAKRI compared to other ISMS standards.

3. Risk management compliance gap analysis

In this research we focus on ISO/IEC 27001 and KATAKRI risk management requirements. Organization may request certification for implemented ISMS against both standards. They both define their own specific set of requirements that ISMS must fulfill to be compliant.

In the preface of KATAKRI it is stated that “the criteria have been created from the perspective of absolute requirements and they do not include a marking system which is used in some criteria”. Also, ISO/IEC 27001 states that “excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.” As both approaches present absolute prerequisite to meet all requirements with yes/no satisfaction criteria, results are comparable by comparing requirements as results are in same scale. Both KATAKRI and ISO/IEC 27001 use the scale of being full compliance or non-compliance. Partial compliance is not accepted. As Karabacak and Sogukpinar (2006) state that the official certification can be difficult as it is “all-or-nothing” design.

The main research question was to analyze is the ISO/IEC audited risk management process compliant with KATAKTRI requirement for risk management. Analysis method was selected to support

bidirectional analysis to see compliance to both of the directions. As result of the analysis we expected to see gap analysis of risk management requirements of ISO/IEC 27001 and KATAKRI. We hope to see that results of this analysis will help organization having either of the certifications to evaluate easier amount of actions required to pursue the other certification.

The risk management requirements are covered in ISO/IEC 27001 in section 4.2.1. There are six main requirements. Three of these requirements contain ten more specific requirements for the corresponding main requirements.

In KATAKRI, risk management requirements are covered in the first part, administrative security. In this part there is subdivision A400, “Identifying, assessing, and controlling risks”. This part contains 12 questions, which each contain several requirements. Risk management requirements are not only limited to section A400, but there are risk management requirements also in other subdivisions of the administrative security main part.

Fenz and Ekelhart (2011) have analyzed five commonly used ISRM methodologies and derived a generic ISRM view out of the selected methodologies. They have created five phases for risk management. Phases and their outputs are represented in table 1.

Table 1: Information security risk management phases and their outputs by Fenz and Ekelhart (2011).

ISRM phases and outputs	
Phase	Output
System characterization	Inventory list of assets to be protected, including their acceptable risk level.
Threat and vulnerability assessment	List of threats and corresponding vulnerabilities endangering the identified assets.
Risk determination	Quantitative or qualitative risk figures and levels for identified threats.
Control identification	List of potential controls that can mitigate the risks to an acceptable level.
Control evaluation and implementation	List of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level.

We identified the risk management requirements from ISO/IEC 27001 and KATAKRI and categorized them into ISRM phases. Content of each category was analysed to find gaps between requirement definitions. Both ISO/IEC 27001 and KATAKRI define requirements to establish risk assessment procedure, which is outside of the scope of ISRM phases. Hence these requirements were analysed as separate set of requirements.

4. Results

This chapter represents key results of the requirement analysis. In the following tables 2 and 3, requirement criteria without corresponding criteria in other specification is presented in *italic* style. Tables don’t include all requirements for clarity, but the most important requirements for all phases are included.

Requirements outside of the scope of ISRM phases set the prerequisites to implement risk assessment methodology, which shall implement requirements categorized into phases. Table 2 represents identified requirements for risk assessment procedures.

Table 2: Risk assessment procedure requirements mapping

Risk assessment procedure requirements mapping	
KATAKRI	ISO/IEC 27001
● Define a risk assessment procedure (A401.0) ● Results of the risk assessment procedure are documented (A401.0) ● *Measure risk assessment process (A407.0)* ● *Risk assessment is performed annually or when significant changes occur (A403/level III) or risk assessment is part of management process (A403/level II)* ● *Results of risk assessment are considered when setting goals of the security work (A404.0)*	● Identify a risk assessment methodology suited to requirements (4.2.1c1) ● Develop criteria for accepting risks (4.2.1c2)

Identified risk management requirements from ISO/IEC 27001 and KATAKRI were mapped to the presented ISRM phases. Results of the mapping are presented in table 3. Corresponding security level is presented in KATAKRI requirements. In addition table includes ISO/IEC 27005 mapping (Fenz 2011).

Table 3: Information security risk management phase mapping

Information security risk management phase mapping			
Phase	KATAKRI	ISO/IEC 27001	ISO/IEC 27005 (Fenz 2011)
System characterization	● Asset identification (A401.1) ● Identify owners of assets (A401.1)	● Identify acceptable levels of risk (4.2.1c2) ● Asset identification (4.2.1d1) ● Identify owners of assets (4.2.1d1)	● Asset identification
Threat and vulnerability assessment	● Threat assessment (A401.1) ● Identify vulnerabilities (I706.0)	● Identify threats (4.2.1d2) ● Identify vulnerabilities (4.2.1d3)	● Identify threats ● Identify vulnerabilities
Risk determination	● Assess risks (A401.2) ● Risks are prioritised (A405.0) ● Likelihood risk estimation (A405.0/level II) ● Risk assessment covers at least security management and personnel, information and premises security (A402.0) ● *Risks relating to external actors are identified (A402.0, A409.0)* ● *Risk assessment influences to security training (A405.0)*	● Identify impact (4.2.1d4, 4.2.1e1) ● Assess threat likelihood (4.2.1e2) ● Assess vulnerability (4.2.1e2) ● Likelihood risk estimation (4.2.1e4)	● Identify impact ● Assess threat likelihood ● Assess vulnerability ● Likelihood risk estimation

Control identification	(No requirements)	● *Identify and evaluate options for the treatment of risks (4.2.1f)*	● Evaluate existing and planned controls
Control evaluation and implementation	● Controls are proportioned to the assets and the relevant risks (A401.1) ● Management approved chosen controls (A401.2) ● Management approval for residual risks (A401.2)	● Select control objectives and controls (4.2.1g) ● Management approval for residual risks (4.2.1h)	● Information security risk treatment (risk avoidance, risk transfer, risk reduction, or risk retention)

As seen from table, KATAKRI does not explicitly require identify and evaluate possible options to mitigate the risks. Rationale for this can be found from the other sections of KATAKRI documentation. Criteria itself contains mandatory controls for each defined security level. Therefore it is not mandatory for organization to evaluate other possible risk treatment options or controls. As ISO/IEC 27001 does not set any specific controls, but only defines normative controls, it is mandatory for organization itself to identify and evaluate appropriate options for risk treatment.

5. Conclusions

Comparing natural language requirements has exposed variety of problems. Many of the analyzed requirements have problems with the completeness. KATAKRI also contains several redundant requirements. Mutual ontology between compared standards facilitates analysis. While KATAKRI is lacking definition of terms, its definitions must be extracted from referred documents. In subdivision A400, “Identifying, assessing, and controlling risks” both ISO/IEC 27001 and 27002 are among the referred documents. Hence risk management terminology is coherent in both documents, but problems exist in other parts of the KATAKRI.

Gap analysis indicates that the KATAKRI certified ISMS implements the most of the risk management requirements of ISO/IEC 27001, but some exceptions exist. As presented in previous chapter, KATAKRI does not have requirement to evaluate and identify possible options for risk treatment. Rationale for this is that KATAKRI itself defines minimum set of controls for each defined security level. ISO/IEC 27001 does not define any mandatory controls, but all controls defined in ISO/IEC 27002 are under considered as normative. The second ISO/IEC 27001 requirement missing from KATAKRI is risk likelihood analysis, which is required by the KATAKRI only on the high security level (level II). KATAKRI requires grouping risks by the importance, but this is not exactly same requirement as likelihood analysis, because risk importance may comprise other risk attributes such as impact. The third difference is the identification of the vulnerabilities. KATAKRI does not require risk management process to identify vulnerabilities, but has requirement to identify the technical vulnerabilities in section of information assurance.

ISO/IEC 27001 certified ISMS does not automatically fulfill all KATAKRI risk management requirements. Following requirements from KATAKRI are not included in ISO/IEC 27001:

1. Risk management process is measured.
2. Risk assessment is performed annually or when significant changes occur (A403/level III) or risk assessment is part of management process (A403/level II).
3. Risk assessment results drive security work.
4. Management has approved chosen controls.
5. Risk assessment is also required, when relevant, from external actors like subcontractors and service providers.
6. Risk assessment influences to security training.

When organization implements ISMS using PDCA model, the requirements for measurement, periodic assessment, results driving security work and management approval for security controls, should be

fulfilled. These are part of “check” and “act” phases of PDCA model to measure results and achieve continuous improval of ISMS.

The other two deviating requirements, “assessing external parties” and “assessment influence to security training” are covered by normative controls in ISO/IEC 27002. Requirement assessing external parties is analogous to “Addressing security in third party agreements”. In ISO/IEC 27002, control “Information security awareness, education, and training” has guideline to include known threats in security training. If this control is implemented, ISMS procedure should also fulfill the KATAKRI requirement.

In this study our target was to compare contents of risk management requirements between ISO/IEC 27001 and KATAKRI. As results show, some deviations between requirements exists to both directions and requirements are not completely overlapping. Major deviation between models is the identification possible options for the risk treatment. Where ISO/IEC 27001 requires organizations to implement a process to identify potential options, KATAKRI defines itself a minimum set of controls for each of the three security levels. Most of the KATAKRI requirements missing from ISO/IEC 27001 are fulfilled when ISMS is implemented using PDCA model. Other deviations in the risk management are minor and a well implemented ISMS should cover these requirements.

6. Discussion

This research was limited to analyzing KATAKRI and ISO/IEC 27001 requirements for risk management. For organizations having either of certifications, it would be meanful to have analysis of complete requirement definitions. Comparison structure should compare each security level from KATAKRI to combination of ISO/IEC 27001 and 27002. As we have seen that some of the KATAKRI requirements are covered in the normative controls of ISO/IEC 27002, which should be included in comparison even it is normative document.

In this study we have identified some problems that KATAKRI currently comprises. One of them is the lack of common ontology over the document. This leaves possibility for interpretation instead of having exact requirements for ISMS. Another identified problem is the natural language requirements. As long as KATAKRI is structured as requirements compliance questionnaire, the problem can only be mitigated enhancing requirement definition quality.

Future research is continued on evaluating existing risks for IT companies and how current ISMS certification models correlate to existing risks. One of the goals is to study if the ISMS certificate will help organizations to find cost-efficient, risk reducing security controls or does certification just cause additional costs for the organization that doesn’t reduce actual risks at all.

References

Baker, W.H. & Wallace, L. 2007, "Is Information Security Under Control?: Investigating Quality in Information Security Management", Security & Privacy, IEEE, vol. 5, no. 1, pp. 36-44.

Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R. & Toval, A. 2011, "Basis for an integrated security ontology according to a systematic review of existing proposals", Computer Standards & Interfaces, vol. 33, no. 4, pp. 372-388.

Boehmer, W. 2009, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001", Availability, Reliability and Security, 2009. ARES '09. International Conference on, pp. 392.

Broderick, J.S. 2006, "ISMS, security standards and security regulations", Information Security Technical Report, vol. 11, no. 1, pp. 26-31.

Fenz, S. & Ekelhart, A. 2011, "Verification, Validation, and Evaluation in Information Security Risk Management", Security & Privacy, IEEE, vol. 9, no. 2, pp. 58-65.

Gandhi, R.A. & Lee, S. 2007, "Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment", Requirements Engineering Conference, 2007. RE '07. 15th IEEE International, pp. 231.

ISO/IEC 27001:2005 2005, Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office, Geneva, Switzerland.

ISO/IEC 27002:2005 2005, Information technology – Security techniques – Information security management systems – Code of practice for information security management, ISO copyright office, Geneva, Switzerland.

Karabacak, B. & Sogukpinar, I. 2006, "A quantitative method for ISO 17799 gap analysis", Computers & Security, vol. 25, no. 6, pp. 413-419.

KATAKRI 2011, National Security Auditing Criteria version II, Ministry of Defence, Finland.

Lee, S., Gandhi, R., Muthurajan, D., Yavagal, D. & Ahn, G. 2006, "Building problem domain ontology from security requirements in regulatory documents", Proceedings of the 2006 international workshop on Software engineering for secure systemsACM, New York, NY, USA, pp. 43.

Pereira, T. & Santos, H. "A Conceptual Model Approach to Manage and Audit Information Systems Security", Proceedings of the 9th European Conference on Information Warfare and Security, Academic Conferences Limited, pp. 360.

Posthumus, S. & von Solms, R. 2004, "A framework for the governance of information security", Computers & Security, vol. 23, no. 8, pp. 638-646.

Siponen, M. & Willison, R. 2009, "Information security management standards: Problems and solutions", Information & Management, vol. 46, no. 5, pp. 267-270.