Comparison of two specifications to fulfill security control objectives

Riku Nykänen,Tommi Kärkkäinen
University of Jyväskylä, Jyväskylä, Finland
riku.t.nykanen@student.jyu.fi
tommi.karkkainen@jyu.fi

Abstract: Assuring information security is a necessity in modern organizations. Many recommendations for information security management (ISM) exist, which can be used to define baseline of information security requirements ensuring that an organization has implemented the selected practices. ISO/IEC 27001 prescribes a process for ISM system and guidance to implement security controls is provided in ISO/IEC 27002. Finnish National Security Auditing Criteria (KATAKRI) has been developed by the national authorities in Finland to verify maturity of information security practices. KATAKRI defines both security control objectives and absolute security controls to meet an objective. ISO/IEC 27001 requires selection of valid security controls whereas KATAKRI may force organization to implement controls that are not feasible from risk management or cost-benefit ratio point of view. In our work, we study differences of the security control objectives and the actual controls of ISO/IEC 27002 and KATAKRI to analyze completeness and mutual coverage between the two specifications. The results reveal the different scope and the lack of some of the controls of KATAKRI compared to ISO/IEC 27001 and ISO/IEC 27002.

Keywords: information security management, ISO/IEC 27001, ISO/IEC 27002, KATAKRI

1. Introduction

Assuring information security is a necessity in modern organizations. There exists variation of viewpoints in information security management (ISM) concerning ‘what’ should be done (ISO/IEC 27000 and COBIT; IT management), ‘how’ it should be done (ITIL; service management), and ‘who’ should do it (SFIA; competence management), see (Armstrong 2013). These recommendations are used to define baseline of information security requirements ensuring that an organization has implemented the selected practices. Some of the recommendations provide the possibility for organizations to request certification, which is can then be granted if the implemented practices fulfill the audition criteria.

Widely adopted ISO/IEC 27001 prescribes a process for ISM system whereas guidance to implement security controls is defined in ISO/IEC 27002. Hence, together they comprise minimum criteria of controls and their objectives, providing also non-normative guidance for control implementation. Finnish National Security Auditing Criteria (KATAKRI) has been developed by the national authorities in Finland to verify maturity of information security practices. Approach in KATAKRI is different compared to ISO/IEC 27000 standards. As national security auditing criteria, KATAKRI defines both security control objectives and absolute security controls to meet an objective. Implementation of controls is mandatory whereas ISO/IEC 27001 leaves responsibility of the selection of controls and their implementation to organization itself by defining only the control objectives. Use of ISO/IEC 27001 is always subject to completeness of risk assessment and selection of valid security controls. On the other hand, KATAKRI may force organization to implement such controls that are not feasible from risk management or cost-benefit ratio point of view.

In our work, we study differences of security control objectives and actual controls of ISO/IEC 27001 and KATAKRI requirements to analyze completeness and mutual coverage of KATAKRI and ISO/IEC 27001. The actual comparison also takes into account ISO/IEC 27002 security control implementation guidelines, creating links between them and the security requirements in KATAKRI. First of all, however, the two specifications are united in their terminology and structure, but whereas ISO/IEC 27002 focuses on existence of security controls to meet the security objectives, KATAKRI defines different levels of requirements that shall be fulfilled. Barlette & Fomin (2008), Fomin et al (2008), Yeniman Yildirim et al (2011), and Siponen (2006) all criticize that information security management standards focus on security process, not how well activities are carried out or how objectives are achieved. To cope with these ISMS hindrances, we create an explicit linking between a process-oriented standards and (normal) operative mode assessment in an organization.

Our analysis of KATAKRI and ISO/IEC 27002 specifications is focused to see the amount of shared common security aspects. In addition, we are interested in differences of the specifications to see the potential gaps in them, especially in the relatively new KATAKRI.

The contents of the paper are as follows: After the introduction, we provide background information on the two specifications and comparative approach in general in Section 2. Then, in Section 3 a structural comparison of specifications and high level comparison of contents of the both specifications is provided. In Section 4, we present more detailed comparison results including intersection and complements of the specifications. In Section 5 we have discussion on the results and further research.

2. Background

2.1 Basic concepts

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. Risk is a combination of the probability of an event and its consequence. Control (countermeasure) is a mean of managing risk, including policies, procedures, guidelines, practices, or organizational structures. Threat is 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, 2005)

2.2 ISO 27000 standards

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.

Appendix of ISO/IEC 27001 and ISO/IEC 27002 itself contain comprehensive list of controls and their objectives. Although ISO/IEC 27001 states that also additional control objectives and controls may be needed and identified from other sources. Organization defines which of the controls it shall implement. Organization may request certification against ISO/IEC 27001 for implemented ISMS. For both ISO/IEC 27001 and 27002 updated versions were released on October 2013.

2.3 KATAKRI – Finnish national security auditing criteria

Another approach to manage corporate security is the 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 the 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)

2.4 Comparing standards and models

Comparing standards or methodologies may reveal several hindrances. One is the lack of widely adopted common ontology containing definitions of the basic concepts and relationships. Ramanauskaite et al. (2013) have identified that major information security management standards utilize only partially comparable security ontologies. Hence, even if standards and methodologies should lead to harmonized ontology definition, there does not exist a single widely adopted ontology definition.

Pardo et al. (2011) emphasize that in comparison it is possible to, using relationships of the models, find out how different the compared models are. Pardo et al. defines that “*in the model comparison the need to know the level of equality and proportion between the things being compared should take the priority*”. One part of comparison is terminology analysis. Pardo et al (2011) divide terminology analysis into two subtypes; syntactic analysis and semantic analysis. Our study uses only semantic analysis as the contents of the compared documents is defined in natural language and require qualitative analysis.

Multiple models can have various types of connections between them. Pardo et al (2011) have identified four operations: union, intersection, difference, and complement. Intersection contains elements that are common

in all the models and union combines together the shared contents. Difference comprises elements that the compared models do not have in common. Complement is a set of elements that are not included in one of the compared models. When comparing only two models, both complements are equal to the difference of the models.

3. Structural view

From structural point of view both ISO/IEC 27001 and KATAKRI controls are divided into logical groups. Following definitions are equal in both, 2005 and 2013, ISO/IEC 27002 standard versions. In ISO/IEC 27002 standard the highest level of grouping is called clauses. Each of these clauses contain "*one introductory clause introducing risk assessment and treatment*" and a number of security categories. Each security category contains one control objective and one or more controls. ISO/IEC 27002:2005 defines that control objective states what is to be achieved. The security controls in the security category can be applied to achieve the control objective. Again ISO/IEC 27002 versions 2005 and 2013 state: "*control defines the specific control statement to satisfy the control objective*". Each control is attached with the implementation guidance, which provides instructions on control implementation to meet the control objective. Definition of the implementation guidance also states that guidance may not be suitable for all organizations and other implementation options can be more appropriate. For each control there is also other information included such as references to other standards or legislation.

KATAKRI is organized as a requirements compliance questionnaire. It has four major sections called divisions, which are divided again into subdivisions. Each subdivision contains number of questions. It defines a number of requirements in the form of questions. Each question consists of a tripartite classification of requirements, corresponding to the security level concepts: the base level (level IV), the increased level (level III), and the high level (level II). These levels correspond to international security level concepts restricted, confidential, and secret, respectively. KATAKRI does not contain requirements for the highest security level, internationally known as top secret (level I).

For the KATAKRI certification the organization shall select the pursued security level. Based on selection, every requirement defined for the selected security level must be complied in each question. In addition to three security levels, there is additional set of requirements as recommendations for the industry. It contains useful security requirements recommended to all businesses to implement. For each level and industry recommendation, a number of requirements is attached. These requirements may be the same for all levels and industry recommendations, they may differ depending on the level, or higher security levels may add more requirements to the base level requirements. The questions and requirements are defined in natural language. For each question there is additional information, containing, for example, references to standards, including ISO/IEC 27002:2005, and implementation guidance.

Where KATAKRI requirements are merely ones that can be answered yes or no, ISO/IEC 27001 auditor has to evaluate that the identified set of security controls is comprehensive and implemented according to the qualitative requirements of the security controls.

ISO/IEC 27002 and KATAKRI both share the same approach grouping security concepts first on high level and then on the secondary level. In ISO/IEC 27002, highest level of grouping is division of security clauses. On the other hand, KATAKRI is divided into four divisions, which are further divided into subdivisions. Table 1 represents ISO/IEC 27002 security clause and the KATAKRI divisions and their subdivisions. ISO/IEC 27002 states that the security clauses are not in specific order concerning prioritization of the security clauses or controls. In KATAKRI prioritization is implemented in dividing security controls based on pursued security level, where the primary controls are defined at the base level. Hence, KATAKRI divisions and subdivisions do not relate to prioritization.

Table 1: ISO/IEC 27001 standard versions 2005 and 2013 security clauses and KATAKRI divisions and subdivisions.

Logical groups of security controls		
ISO/IEC 27001:2005	ISO/IEC 27001:2013	KATAKRI
1. Security policy 2. Organization of information security 3. Asset	1. Information security policies 2. Organization of information security	1. Administrative security 1.1. Security policy, the measures guiding security action and definitions 1.2. The annual security action programme 1.3. Defining the goals of security

management 4. Human resources security 5. Physical and environmental security 6. Communications and operations management 7. Access control 8. Information systems acquisition, development and maintenance 9. Information security incident management 10. Business continuity management 11. Compliance	3. Human resource security 4. Asset management 5. Access control 6. Cryptography 7. Physical and environmental security 8. Operations security 9. Communications security 10. System acquisition, development and maintenance 11. Supplier relationships 12. Information security incident management 13. Information security aspects of business continuity management 14. Compliance	1.4. Identifying, assessing and controlling risks 1.5. Security organisation and responsibilities 1.6. Accidents, danger situations, security incidents and preventive measures 1.7. Security documentation and its management 1.8. Security training, increasing awareness and knowhow 1.9. Reports and inspections by the management 2. Personnel Security 2.1. Technical criteria 2.2. Securing sufficient competences 2.3. Other suitability of the candidate for the task 2.4. Measures after the decision to recruit 2.5. Measures for concluding the contract of employment 2.6. Measures during employment 3. Physical Security 3.1. Security of area 3.2. Structural security 3.3. Security technical systems 4. Information assurance 4.1. Data Communications Security 4.2. Security of Information Systems 4.3. Security of Information 4.4. Security of Information Handling

UML class diagram of the structures of the both documents is presented in the Figure 1. ISO 27002 standards structure is equal in both version of the standard and it contains definition of terms and their relationships. KATAKRI, on the other hand, does not contain ontology definition at all. Hence, we identified basic structures of the KATAKRI document.

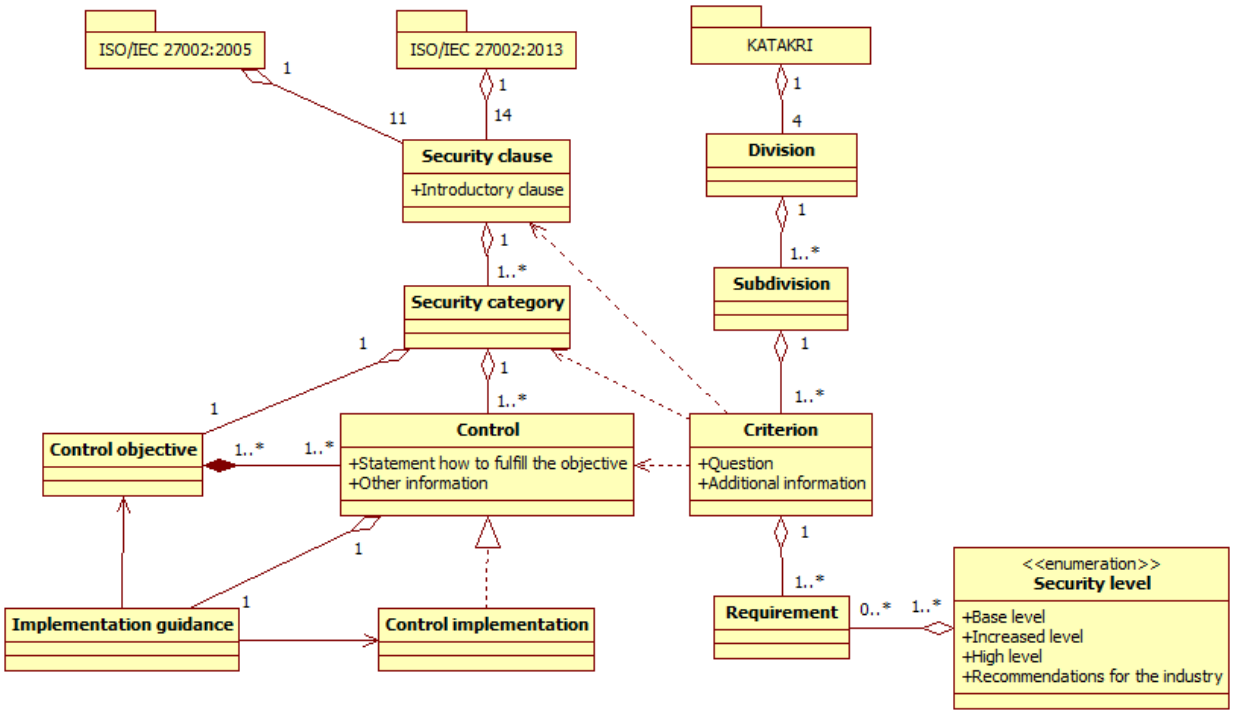

Figure 1: UML class diagram presenting structures of ISO/IEC 27002 and KATAKRI

Even if ISO/IEC 27002 and KATAKRI both share the same approach of grouping security concepts on high level, the actual structures have significant differences at lower levels. ISO/IEC 27002 standard defines control objective, which shall be achieved by implementing the defined controls. KATAKRI, on the other hand, has a question that is answered, fulfilling requirements defined for the question of the corresponding security level. Hence, KATAKRI question and ISO/IEC 27002 control objective both set goal, which is achieved by implementing defined controls or requirements.

ISO/IEC 27002 contains implementation guidance for each control that it defines. Actual implementation of the control can be done as specified in the implementation guidance or organization can select an approach that suits to its needs and characteristics (ISO/IEC 27002:2013). KATAKRI does not contain implementation guidance but provides additional information such as references to standards, legislation, and security guides.

We analyzed all requirements of the KATAKRI and identified matching definitions from ISO/IEC 27002:2005. In addition we also counted number of references from KATAKRI to ISO/IEC 27002:2005. As KATAKRI defines also requirements for risk management, we included risk management requirements of ISO/IEC 27001:2005 in the analysis.

In general, the results reveal that KATAKRI had in total 432 connections to the ISO/IEC 27002:2005. From these connections 91 were direct references to ISO/IEC 27002:2005. One of these direct references is to security clause, 16 to security categories, and 74 to security controls. KATAKRI requirements had semantic equality with 21 controls. The most of the connections were semantic equality of KATAKRI requirements to implementation guidance, which we identified 320. In addition, we found out 20 connections from KATAKRI requirements to risk management section of ISO/IEC 27002:2005 and risk management requirements in ISO/IEC 27001:2005. Hence total number of identified connections was 452. Summary matrix of the connections between ISO/IEC 27002:2005 security clauses and the KATAKRI divisions is included in the appendix 7.1 and Figure 2.

4. Operational view

We have divided the more specific results into four groups. First we present intersection of the two specifications. These are security controls that exist in both documents. Then we present complements of both ISO/IEC 27002 and KATAKRI, which discloses differences of the documents. More precisely, Section 4.2 contains security topics that are contained in ISO/IEC 27002 but not in KATAKRI and Section 4.3 contains the ones that are in KATAKRI but not in ISO/IEC 27002. We close the section by presenting other findings from the documents.

4.1 Intersection of specifications

In the general documents have sections that contain same topics, which can be seen as high number of links between security clauses and KATAKRI divisions as presented in the Figure 2: Number of connections between ISO/IEC 27002:2005 security clauses and KATAKRI divisions. Numbering is as presented in Table 1, not as security clauses are numbered according chapters in ISO/IEC 27002:2005 specification. The general security management in ISO/IEC 27002:2005 as defined in the security clauses (1-4) and (10-11) is strongly linked to KATAKRI's first division 'Administrative security'. Similarly, 'Personnel security' in KATAKRI and 'Human resource security' in ISO/IEC 27002:2005 are linked but not very strongly. Also the areas of physical security (6 in ISO/IEC 27002:2005 and 3 in KATAKRI) are connected. The fourth division, 'Information assurance' in KATAKRI is much dispersed related to ISO/IEC 27002:2005 covering both concrete areas in security operations (6-9) as well as higher level operations management (11-12).

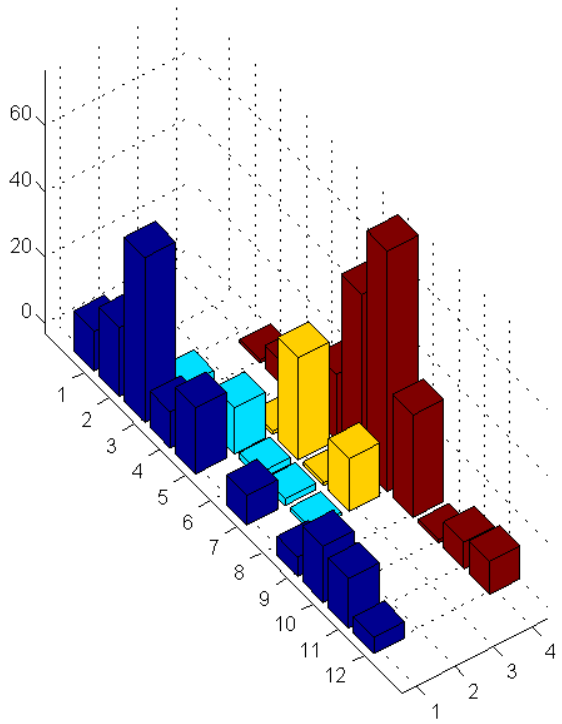

Figure 2: Number of connections between ISO/IEC 27002:2005 security clauses and KATAKRI divisions.

In detail, several common topics that were covered by both ISO/IEC 27002 and KATAKRI were identified. Following Table 2: Intersection of ISO/IEC 27002 and KATAKRI presents intersection of the specifications divided into four domains defined by the KATAKRI.

Table 2: Intersection of ISO/IEC 27002 and KATAKRI

Common topics of information security in ISO/IEC 27002 and KATAKRI	
	Common topics
Administrative security	• Security policy (22 connections) • Risk management (52 connections) • Security organization and responsibilities (26 connections) • Incident management (8 connections) • Business continuity management (32 connections)
Personnel security	• Security training (36 connections) • Contracts with employee (8 connections) • Termination of contract (6 connections)
Physical security	• Structural security (19 connections) • Physical access control (26 connections)
Information security	• Communication security (31 connections) • Information access control (26 connections) • Malware prevention and vulnerability management (12 connections) • Logging (10 connections) • Unauthorized devices (7 connections) • Encryption (6 connections) • Security of executable code (9 connections) • Handling of classified information (24 connections) • Systems management (10 connections) • Remote work/teleworking (28 connections) • Separation of production and development environments (8 connections) • Backup (10 connections

The highest number of connections was in risk management as both methods require same approach to identify assets and threats to assets to perform risk mitigation. Both specifications keep security training and rising of the security awareness as an important aspect of information security.

4.2 ISO/IEC 27002 complements

We identified that KATAKRI contained in total only nine connections to ISO/IEC 27002:2005 security categories “12.1 Security requirements of information systems” and “12.2 Correct processing in applications“. These two security categories contain requirements for new information system development and only nine links is relatively small amount to cover all requirements for the information system development. In the ISO/IEC 27002:2013 “12.1 Security requirements of the information systems” has been updated and category number has been changed to 14.1. Section “12.2 Correct processing in applications“ and controls of it in ISO/IEC 27002:2005 have been removed from version 2013. These have been complemented with two new controls in section 14.1 of the 2013 version, but KATAKRI don’t have wider correlation to either of these. Rationale for this is that KATAKRI is not meant to provide requirements for information system development, because it is audition criteria. Actually a security guideline for information system development in the state institutions, called “VAHTI 1/2013 Sovelluskehityksen tietoturvaohje“, has been published. This guideline covers security requirements for the information system development. Problem has been identified also in Finnish Defence Forces in the thesis by Liitsalo (2013) where she concludes that VAHTI 1/2013 has fulfilled the lack of common national guideline of generic information system development security requirements.

ISO/IEC 27002:2005 contains one security category, “10.9 Electronic commerce services”, where we did not identify any links from KATAKRI. This category and contained controls have been removed from ISO/IEC 27002:2013. At the time ISO/IEC 27002:2005 was published electronic commerce was emerging and it was seen as an important domain to cover. As time passed, there are many other information systems available through the internet. Hence, electronic commerce services have become only a one type among other services provided in internet, which all need to consider security in the cyber age.

ISO/IEC 27002:2013 contains controls to gather evidence in case of security incident. In KATAKRI one finds very limited requirements to cover evidence collection in case of security incidents. The KATAKRI requirements merely focus to protect audit trails, but don’t include additional requirements to collect and secure the evidence.

Further complementing area in ISO/IEC 27002, compared to KATAKRI, was reporting of security weaknesses. The ISO/IEC 27002 has a specific control (13.1.1 in version 2005 and 16.1.3 in version 2013) to emphasize employee responsibility report observed or suspected security weaknesses and vulnerabilities. KATAKRI does not contain requirement that would highlight employee responsibility to report weaknesses, even if it clearly states that for each employee the security responsibilities must be defined in their job description.

The compliance was an area where the level of details varied between specifications. Where ISO/IEC 27002 provides implementation instructions types for compliance and how to achieve compliance, KATAKRI has only the basic requirement that all operations must be compliant according to legislation.

4.3 KATAKRI complements

KATAKRI has some topics that are not part of ISO/IEC 27002 standards. On the administrative security KATAKRI contains the concept of annual security action programme, which is covered in KATAKRI subdivision A200. It is an annual plan how security will be developed comprising measures, responsibilities, schedules, and measurable results. The results of the implementation of the plan are expected to be monitored by the management as continuous process. It is notable that there are no requirements for annual security programme at the base level, but they are included in the recommendations for the industry.

We identified number of requirements in KATAKRI that require documentation of the performed actions, but did not find equal control from ISO/IEC 27002 control objective or implementation guidance. One such topic was training, where KATAKRI requirement define that the arranged trainings must be documented, including training material and participants. ISO/IEC 27002 controls have similar control to raise awareness, but implementation guidance does not cover documentation of training. Similar widely used documentation requirement was is a job description, which is in several KATAKRI requirements referred as written definition of the responsibilities of an employee.

KATAKRI complements ISO/IEC 27002 on high security requirements. KATAKRI contains requirements that must be fulfilled to be able to handle material that is classified secret by the Finnish national definition. For the organizations that don't consider information security as competitive advantage, these controls may not be feasible to implement. These controls don't have high cost-benefit-ratio and are valid only in security critical businesses.

Hence, KATAKRI is Finnish national security audition criteria and it contains also requirements that may be illegal in other countries. Such requirements are drug tests and probationary period used in recruitment. KATAKRI also contains national requirements for physical security alarms. Such requirements are not included in the ISO/IEC 27002 standard.

4.4 Additional results

We found out also more than 20 major translation errors in KATAKRI (original version is in Finnish, which is translated to English), where a translation error caused difference in requirements. For example, in some criterions there was for certain security level "No requirements" in English version, but the original Finnish version did contain requirements.

5. Discussion

In our study we analyzed ISO/IEC 27002 versions 2005 and 2013 and compared them to Finnish security audition criteria, KATAKRI. We found out that both contain largely same security controls that security aware organizations should implement, but under a completely different structural division. Analysis also illustrates evolution of information security management trends. Results can be applied in upcoming versions of KATAKRI to evaluate the overall scope and boundaries of the security controls. They are equally relevant for ISO/IEC standardization, even if a refined version already appeared in 2013.

We identified number of common security topics that we covered by the both of the specifications. The results reveal the different scope and lack of some of the controls of KATAKRI compared to ISO/IEC 27001 and ISO/IEC 27002. Moreover, normative controls of the KATAKRI were detected, which are not included even as implementation guidance in ISO/IEC 27002.

It has been noticed that SMEs have to focus more on development of their information security procedures, but most of the ISMS standards are not usable from SME organization point of view. For example, ISO/IEC 27001 has been criticized being too large and complicated to be adopted with the resources of SMEs. While SMEs struggle with limited resources, but increasing threads, it is important to develop new approaches that suit especially for SMEs. Majority of modern information security management systems are developed for at least medium sized enterprises. One question driving our future study is: "we have firewall and antivirus software, but what next?"

KATAKRI contains basic prioritization of the security requirements as all the requirements have been defined for three information classification levels and in addition there are recommendations for the industry. ISO/IEC 27002 in the other hand states in the document that security controls are not in any means prioritized. In the KATAKRI, even at the lowest security level (or only even the recommendations for the industry), amount of controls is out reach for SMEs where security is not strategic competence area. For example, the NIST standard 800-53 (2009) defining recommended security controls for the federal information systems and organizations, contains prioritization of the security controls.

In addition we plan to include viewpoints for organization types and personnel roles to security tools. Where current document-based approaches are rigid to separate interesting topics of different job functions, some modern presentation methods, like wiki-format, may be more usable.

6. References

Armstrong, C.J. 2013, "An Approach to Visualising Information Security Knowledge" in *Information Assurance and Security Education and Training*, Springer Berlin Heidelberg, pp. 148-155.

Barlette, Y. & Fomin, V.V. 2008, "Exploring the Suitability of IS Security Management Standards for SMEs", *Hawaii International Conference on System Sciences*, Proceedings of the 41st Annual, pp. 308.

Fomin, V.V., de Vries, H.J. & Barlette, Y. 2008, "ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption", *EUROMOT 2008 Conference*, Nice, France.

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

ISO/IEC 27001:2013 2013, *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.

ISO/IEC 27002:2013 2013, *Information technology - Security techniques - Information security management systems - Code of practice for information security management*, ISO copyright office, Geneva, Switzerland.

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

NIST Special Publication 800-53 2009, *Recommended Security Controls for Federal Information Systems and Organizations,* National Institute of Standards and Technology.

Pardo, C., Pino, F.J., García, F., Piattini, M. & Baldassarre, M.T. 2012, "An ontology for the harmonization of multiple standards and models", *Computer Standards & Interfaces*, vol. 34, no. 1, pp. 48-59.

Ramanauskaite, S., Olifer, D., Goranin, N. & Cenys, A. 2013, "Security Ontology for Adaptive Mapping of Security Standards", *International Journal of Computers Communications & Control*, vol. 8, no. 6, pp. 878-890.

Siponen, M. 2006, "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, vol. 49, no. 8, pp. 97-100.

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

Yeniman Yildirim, E., Akalp, G., Aytac, S. & Bayram, N. 2011, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey", *International Journal of Information Management*, vol. 31, no. 4, pp. 360-365.

7. Appendix

7.1 Total number of connections

ISO 27002:2005 and KATAKRI comparison summary (c) Riku Nykänen, 2013-2014 Total number of connections.	Administrative security	Personnel security	Physical Security	Information Assurance	
ISO 27001	8	0	0	0	8
4.Risk assessment and treatment	12	0	0	0	12
5. Security policy	21	0	0	0	21
6. Organization of information security	50	5	0	1	56
7 Asset management	11	1	0	7	19
8 Human resources security	20	14	1	1	36
9 Physical and environmental security	0	2	31	20	53
10 Communications and operations management	9	2	1	52	64
11 Access control	0	1	16	73	90
12 Information systems acquisition, development and maintenance	6	0	0	31	37
13 Information security incident management	17	0	0	1	18
14 Business continuity management	15	0	0	8	23
15 Compliance	5	0	0	10	15
Total	174	25	49	204	452