International Journal of Cyber Warfare and Terrorism

April-June 2014, Vol. 4, No. 2

Table of Contents

Research Articles

The *International Journal of Cyber Warfare and Terrorism* is indexed or listed in the following: Bacon's Media Directory; Cabell's Directories; INSPEC; MediaFinder; ProQuest Advanced Technologies & Aerospace Journals; ProQuest Computer Science Journals; ProQuest Illustrata: Technology; ProQuest Military Collection; ProQuest SciTech Journals; ProQuest Technology Journals; The Index of Information Systems Journals; The Standard Periodical Directory; Ulrich's Periodicals Directory

Aligning Two Specifications for Controlling Information Security

Riku Nykänen, University of Jyväskylä, Jyväskylä, Finland

Tommi Kärkkäinen, University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

Assuring information security is a necessity in modern organizations. Many recommendations for information security management exist, which can be used to define a baseline of information security requirements. ISO/IEC 27001 prescribes a process for an information security management 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 as a tool to verify maturity of information security practices. KATAKRI defines both security control objectives and security controls to meet an objective. Here the authors compare and align these two specifications in the process, structural, and operational level, focusing on the security control objectives and the actual controls. Even if both specifications share the same topics on high level, the results reveal the differences in the scope and in the included security controls.

Keywords: *Information Security, ISO/IEC 27001, ISO/IEC 27002, KATAKRI, Security Audit Criteria, Security Cerification, Security Controls, Security Management, Security Specification Alignment*

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 can then be granted if the implemented practices fulfill the audition criteria.

Widely adopted ISO/IEC 27001 prescribes a process for information security management system (ISMS) 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 in an organization. Approach

DOI: 10.4018/ijcwt.2014040104

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 the 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 benefit-cost ratio point of view.

KATAKRI is of interest for wider than just the national audience because of its structure. It has been created in the form of the audition questionnaire, which makes it a tool that can be used to check the security baseline of an organization. As information security is a process, to protect information and information infrastructure from unauthorized access, a baseline must be defined and evaluated. ISO/IEC 27001 and 27002 specifications are not usable as audition tools themselves and, hence, a number of spreadsheets and special applications have been created from different viewpoints to be used in the auditions. At the topic level, KATAKRI could also be used as an ISO/IEC 27001 audition tool, but this requires detailed analysis and alignment of the correspondences of the two specifications.

In our work, we study differences of security control objectives and actual controls of ISO/IEC 27001 and KATAKRI's 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. More precisely, our analysis of KATAKRI and ISO/IEC 27002 specifications is focused on both shared common security aspects and the actual differences to see the potential gaps in them, especially in the relatively new 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 should 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 information security management system hindrances, we created an explicit alignment between the process-oriented standard and the (normal) operative mode assessment in an organization.

The contents of the paper are as follows: After the introduction, we provide background information on the two specifications and introduce the comparative approach in general in Section 2. Comparison of certification and accreditation processes in the two specifications is provided in Section 3. Then, in Section 4, a structural comparison and alignment of the two specifications, providing a common terminology, and high level comparison of their contents is performed. In Section 5, we present more detailed comparison results including intersection and complements of the specifications. Related work is presented in Section 6. Finally, in Section 7, conclusions and discussion on the results is provided and further research needs pointed out.

2. BACKGROUND

2.1. 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 detailed controls with implementation guidelines are presented in ISO/IEC 27002.

Appendix of ISO/IEC 27001 and ISO/IEC 27002 itself contain a comprehensive list of security controls and their objectives. However, ISO/IEC 27001 states that also additional security control objectives and controls may be needed and can be identified from other sources. Organization defines which of the security controls it shall implement. These are part of the ISMS which, then, can be certified against ISO/IEC 27001. For both ISO/IEC 27001 and 27002, updated versions were released on October 2013. The changes in the updates compared to the previous versions included additions of 11 new controls, but the total number of the controls was decreased from 133 to 114. Some of the earlier controls were removed and some were merged together. The number of the highest level groups of controls, security clauses, was increased from 11 to 14.

2.2. KATAKRI: Finnish National Security Auditing Criteria

Another approach of interest 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. The initial version of KATAKRI was published in 2009 and the updated second version in 2011.

The first goal of the national security auditing criteria is to harmonize official measures while assessing organization's 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, the documentation also contains unofficial recommendations to help users to apply useful security practices. (KATAKRI, 2011)

KATAKRI defines requirements operating in three different levels of security: the base level (IV), the increased level (III), and the high level (II). The levels correspond to the international security level classification as *restricted, confidential, and secret*, respectively. KATAKRI does not contain requirements for the highest security level (I), internationally known as the *top secret*. Based on the need of the handled information classification, audition requirements vary. Where the focus of the base level is to assess the foundation of security management and implemented security controls, the high level includes requirements to minimize the security risks.

2.3. Comparing Standards and Models

Comparison of standards or methodologies may reveal several hindrances. One is the lack of widely adopted common ontology containing definitions of the basic concepts and their relationships. This goes beyond the common terminology that was provided in the previous section. 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 a comparison is the terminology analysis. Pardo et al (2011) divide the 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, hence, the comparison inevitably requires 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

Table 1. Summary of common certification and audition terminology

Term	Description	Source
Attestation	issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated	ISO/IEC 17000:2004
Audit	systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the Audit criteria are fulfilled	ISO/IEC 27000:2014
Audit criteria	set of policies, procedures or requirements used as a reference against which Audit evidence is compared	ISO 19011:2011
Audit evidence	records, statements of fact or other information relevant to the Audit criteria and can be verified	ISO 19011:2011
Audit scope	extent and boundaries of an Audit	ISO/IEC 27000:2014
Certificate	certificate issued by a Certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement	ISO/IEC 27006:2011
Certification	third-party Attestation related to products, processes, systems or persons	ISO/IEC 17000:2004
Certification body	third party that assesses and certifies the ISMS of a client organization with respect to published ISMS standards, and any supplementary documentation required under the system	ISO/IEC 27006:2011

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. In this study, we focus on the intersection and complements of the two specifications under consideration.

3. PROCESS ALIGNMENT

3.1. Certification and Audition Terminology

To be able to compare the certification and audition processes, we need to have a common terminology. In Table 1, the key terminology of the common audition and certification concepts of the two specifications is presented. As KATAKRI does not contain terminology definitions, the concepts are derived from relevant ISO/IEC standards ISO/IEC 17000 (2004), ISO 19011 (2011), ISO/IEC 27000 (2014), and ISO/IEC 27006 (2011).

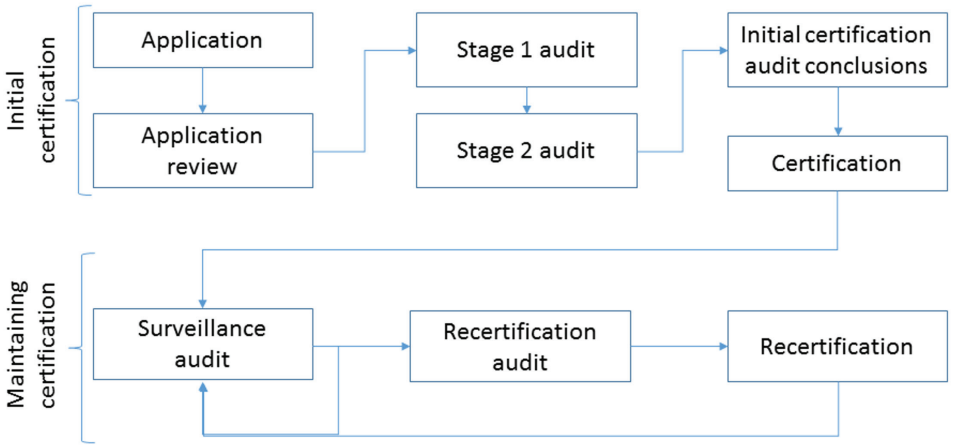
Table 1 excludes terms and definitions related to accreditation of certification bodies, because this is out of the scope of the current comparison.

3.2. Process Stakeholders

ISO, as standardization organization, does not provide the certification of standards developed by it. It does not, either, perform accreditation of the certification bodies, which are accredited by the national accreditation bodies. An organization aiming to receive ISO 27001 certification can select any certification body, with the national accreditation, to perform the actual certification process.

KATAKRI is used by number of public authorities in Finland, like Finnish Defense Forces, to audit their suppliers. Authorities use their own or third-party auditors to perform the auditions. The first target of the KATAKRI is to provide harmonized security requirements shared by all the authorities (KATAKRI, 2011). It is also recommended in the KATAKRI that it should be used by the organizations to self-

Figure 1. ISO/IEC 17021 certification process



assess maturity of their security management and operations.

3.3. Process Comparison

ISO/IEC 27001 certification process requirements, among other ISO standards, are defined in the ISO/IEC 17021:2011 standard "Conformity assessment - Requirements for bodies providing audit and certification of management systems". The standard is prepared by ISO Committee on conformity assessment (CASCO), which is responsible for the development of International Standards and Guides in the field of conformity assessment.

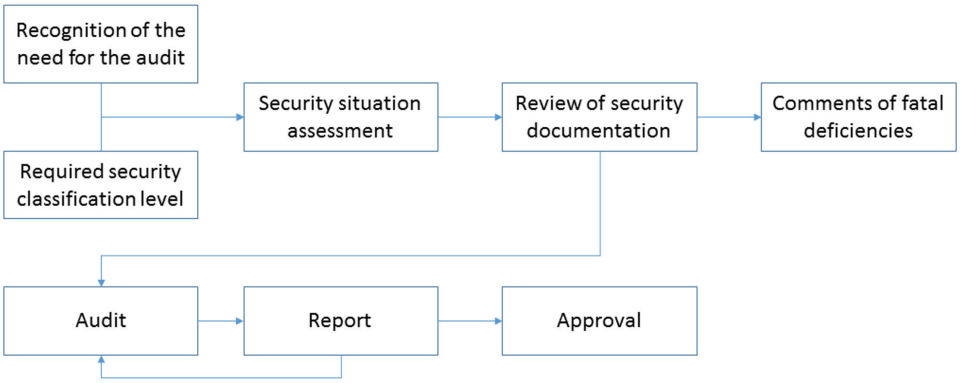
Certification process defined by the ISO/IEC 17021 is started by the organization aiming for certification. The organization submits an application to a certification body. Certification body reviews the application and determines the competences required from an audit team, providing also the final certification decision. The actual certification audition is implemented in two stages. Stage 1 audit focuses on the management system and documentation. Stage 2 audit shall evaluate the implementation of the management system comparing audit evidence to audit criteria. Nonconformities from audits are communicated to client organization and client organization shall provide corrective actions. Audit results from both stage audits and corrective actions are evaluated to determinate whether the certificate can be granted or not.

When an organization has successfully obtained certification, the surveillance audits are performed at least annually to evaluate its capability to maintain the level of operation that fulfils the certification requirements. Surveillance audits are partial and don't cover complete management system. The recertification audit is performed in every three years, which covers the complete information security management system as a whole. When an organization has successfully maintained the required level of operation, certification shall be renewed.

KATAKRI, on the other hand, does not have any specific enforced ways to carry out the certification process, but KATAKRI (2011) document describes an example process for certification. The example process is represented in Figure 2.

KATAKRI certification process is initiated by the recognition of the need for the audit. When the need is recognized, the required security classification level is defined. As KATAKRI supports multiple security classification levels, the audit criteria depend on the select level. In the first phase, the security situation is assessed to build an overall image of the security level.

Figure 2. KATAKRI example certification process. (Adapted from KATAKRI, 2011)



Next, auditors review the security documentation and optionally provide feedback on the fatal deficiencies. The last two activities correspond to Stage 1 audit in ISO/IEC 17021.

After the documentation review, actual onsite audit is performed, similarly to Stage 2 audit in ISO/IEC 17021. Audit results are documented in the audit report. If fatal deficiencies are found, then these are reported and re-audit is performed after corrective actions. When a successful audit is completed, certification can be granted, depending on the accreditation level of the auditor. KATAKRI is used, for example, to provide Facility Security Clearance, which can be required for participation to international tender.

Even if the certification processes of ISO/IEC 27001 and KATAKRI deviate, they still consist of the same components. Key parts of the both processes are documentation review and onsite audition of the actual implementation of the information security management system. Both processes depend on the results of these audits, and corrective actions to overcome the potential deficiencies are verified during the additional audits. ISO/IEC 17021 process covers also maintaining of the certification, where example process of KATAKRI certification terminates to initial certification.

4. STRUCTURAL ALIGNMENT

4.1. Towards Common Terminology

In order to compare the structures of the two specifications, a common overall terminology on the security standard domain would be useful as, e.g., stated by Beckers et al. (2014). KATAKRI does not contain terminology definitions, but contains in total 90 references to ISO/IEC 27000 standards, which is more than to any other international standard. Hence, KATAKRI terminology can be verified in these sections to be comparable to ISO/IEC 27000 terminology. In ISO standards, however, the terminology definitions are distributed over number of referenced standards.

We summarize the security management terminology based on the three ISO standards (ISO 55000:2014, ISO/IEC 27000:2014, ISO/Guide 73:2009) in Table 2.

4.2. Structural Comparison

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 a clause. Each of

Table 2. Summary of common security standard terminology

Term	Description	Source
Asset	item, thing or entity that has potential or actual value to an organization	ISO 55000:2014
Availability	being accessible and usable upon demand by an authorized entity	ISO/IEC 27000:2014
Confidentiality	to not make information available or disclosed to unauthorized individuals, entities, or processes	ISO/IEC 27000:2014
Control	measure that is modifying risk	ISO/Guide 73:2009
Control Objective	statement describing what is to be achieved as a result of implementing controls	ISO/IEC 27000:2014
Information Security Incident	single or a series of unwanted or unexpected information security events that can compromise business operations and threaten information security	ISO/IEC 27000:2014
Integrity	to safeguard the accuracy and completeness of Assets	ISO/IEC 27000:2014
Stakeholder	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity	ISO/Guide 73:2009
Vulnerability	weakness of an Asset or Control that can be exploited by one or more Threats	ISO/IEC 27000:2014
Threat	potential cause of an unwanted incident, which may result in harm to a system or organization	ISO/IEC 27000:2014
Attack	attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an Asset	ISO/IEC 27000:2014
Objective	result to be achieved	ISO/IEC 27000:2014
Requirement	need or expectation that is stated, generally implied or obligatory	ISO/IEC 27000:2014
Risk	effect of uncertainty on Objectives	ISO/Guide 73:2009
Conformity	fulfilment of a requirement	ISO/IEC 27000:2014
Policy	intentions and direction of an organization as formally expressed by its top management	ISO/IEC 27000:2014

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 (see Table 3). The security controls in the security category can be applied to achieve the control objective. Each control is attached with the implementation guidance, which provides instructions on implementing the control 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 further divided into subdivisions. Each subdivision contains number of questions. Hence, a number of requirements are defined in the form of questions. Each question consists of a tripartite classification of requirements, corresponding to the security level (the base level/IV, the increased level/III, and the high level/II).

For the KATAKRI, the organization to be certified shall select the pursued security level. Based on the selection, every requirement defined for the selected security level must be complied in the each question assessing it. In addition to three security levels, there is addi-

Table 3. ISO/IEC 27001 standard versions 2005 and 2013 security clauses and KATAKRI divisions and subdivisions

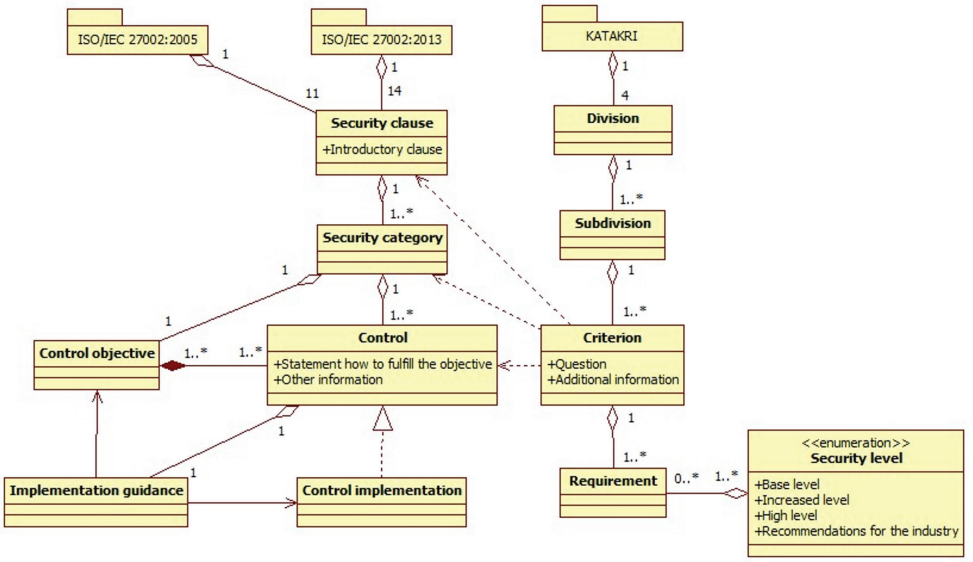
Logical Groups of Security Controls		
ISO/IEC 27001:2005	**ISO/IEC 27001:2013**	**KATAKRI**
1. Security policy 2. Organization of information security 3. Asset management 4. Human resources security 5. Physical and environmental security 6. Communications and operations management 7. Access control 8. Information systems acquisition, development and maintenance 9. Information security incident management 10. Business continuity management 11. Compliance	1. Information security policies 2. Organization of information security 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. 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 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

tional set of requirements as recommendations for the industry. They contain useful security requirements, recommended to all businesses to implement. For each level and industry recommendation, a number of requirements are 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. All the questions and requirements are defined in natural language. For each question, additional information is provided, containing, for example, references to standards, including ISO/IEC 27002:2005, and implementation guidance.

Where KATAKRI requirements are merely the 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 the high level and then on the secondary level. In ISO/IEC 27002, highest level of grouping is the division of security clauses. On the other hand, KATAKRI is divided into four divisions, which are further divided into subdivisions. Table 3 represents ISO/IEC 27002 security clause and the KATAKRI divisions and their subdivisions. ISO/IEC 27002 states

Figure 3. UML class diagram presenting structures of ISO/IEC 27002 and KATAKRI



that the security clauses are not in any specific order concerning prioritization of the security clauses or controls. In KATAKRI, prioritization is implemented in dividing the security controls based on the pursued security level. Hence, KATAKRI divisions and subdivisions do not relate to prioritization.

UML class diagram of the structures of the both documents is presented in Figure 3. ISO 27002 standards structure is equal in both versions of the standard and it contains definition of the 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.

Even if ISO/IEC 27002 and KATAKRI both share the same approach of grouping security concepts on the high level, the actual structures have significant differences at the 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, in order to fulfill requirements on the corresponding security level. Hence, KATAKRI question and ISO/IEC 27002 control objective both set a 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.

4.3. Identified Relationships

We analyzed all requirements of 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 ISO/IEC

27002:2005. From these connections, 91 were direct references to ISO/IEC 27002:2005. One of these direct references is to the security clause, 16 to the security categories, and 74 to the security controls. KATAKRI requirements had semantic equality with 21 controls. Most of the connections were semantic equality of KATAKRI requirements to the implementation guidance. Total of 320 of such links were identified. In addition, we found out 20 connections from KATAKRI requirements to the risk management section of ISO/IEC 27002:2005 and risk management requirements in ISO/IEC 27001:2005. Hence, the 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 Appendix 9.1.

4.4. Implications of the Different Structures

Information security management system based on ISO/IEC 27001 and 27002 is always a risk evaluation driven approach. Even though number of controls is defined in ISO/IEC 27002 specification, implementation of the controls is always a matter of evaluating suitability and appropriateness to the organization. Structurally ISO/IEC 27002 control implementation guidance provides help to implement a proper control, but this still requires expertise from the user. The lack of the competence has been identified as one of the key obstacles to adopt ISMS by Yeniman et al (2011) and especially in small and medium sized enterprises by Barlette & Fomin (2008).

Weiss (2008) identifies two existing questions when evaluating security controls for the organization. First, how effective the current security controls of the organization are? And secondly, how efficient is the investment on the security controls? Security baseline analysis provides answer to the first question, but the latter requires organization specific risk assessment and analysis to be properly answered.

KATAKRI, in comparison to ISO/IEC 27002, provides more exact security requirements to be fulfilled and leaves fewer options to the organization to determine appropriate way to implement the security controls. The approach of the KATAKRI may lead to a situation where the requirements force organization to implement the security controls that are not feasible or have low benefit-cost ratio. Although KATAKRI requirements are more structured and specific, it does not imply that they could be neither implemented nor evaluated with lesser expertise than the ISO/IEC 27002 security controls.

5. OPERATIONAL ALIGNMENT

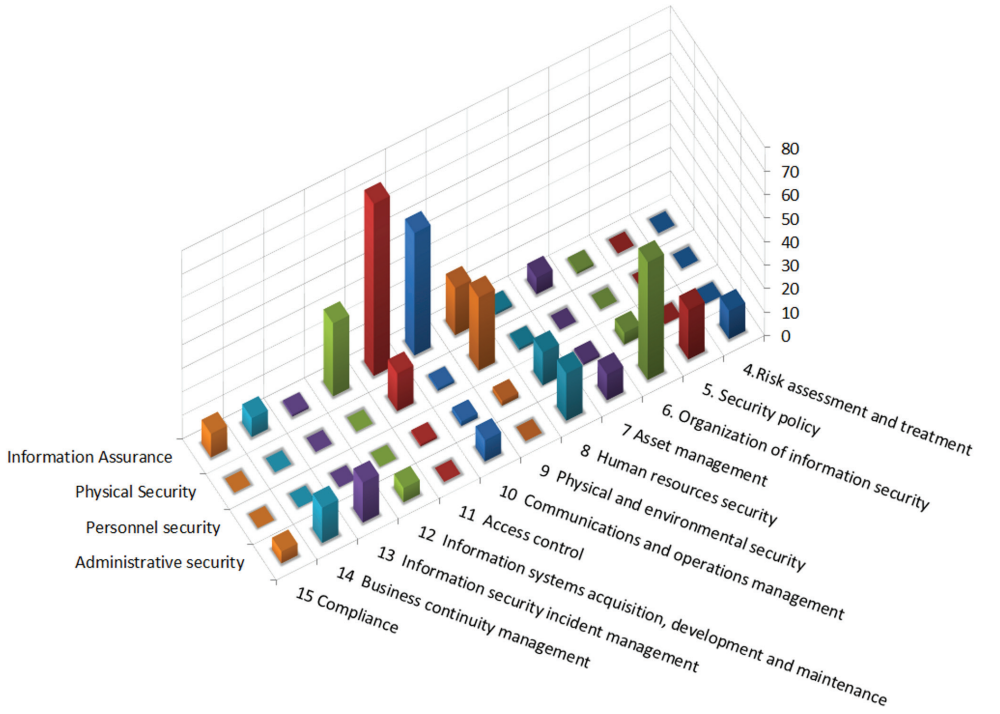
We have divided the more specific results into four groups. First, we present the intersection of the two specifications. This consists of the security controls that exist in the both documents. Then, we present the complements of both ISO/IEC 27002 and KATAKRI, which discloses the differences of the documents. More precisely, Section 5.2 contains those security topics that are contained in ISO/IEC 27002 but not in KATAKRI and Section 5.3 contains the ones that are in KATAKRI but not in ISO/IEC 27002. We close the section by presenting other findings from the two documents.

5.1. Intersection of Specifications

In general, both documents have sections that contain the same topics, which can be seen as high number of links between the security clauses in ISO/IEC 27002:2013 and the division of KATAKRI into subdivisions as presented in Figure 4.

The general security management in ISO/IEC 27002:2005 as defined in the security clauses (4-8) and (14-15) 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 are connected. The fourth division, 'Information assurance', in KATAKRI is much dispersed related to ISO/IEC 27002:2005 covering both

Figure 4. Number of connections between ISO/IEC 27002:2005 security clauses and KATAKRI divisions



concrete areas in security operations (9-12) as well as higher level operations management (14-15).

In detail, several common topics that were covered by both ISO/IEC 27002 and KATAKRI were identified. Table 4 below presents the intersection of the specifications divided into four domains defined by the KATAKRI.

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

5.2. 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 a 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 the controls of it in ISO/IEC 27002:2005 have been removed from the next version in 2013. These have been complemented with two new controls in Section 14.1 of the 2013 version, but KATAKRI doesn't have wider correlation to either of these. Rationale for this is that KATAKRI is not meant to provide requirements for the information system development,

Table 4. Intersection of ISO/IEC 27002 and KATAKRI

Common Topics of Information Security in ISO/IEC 27002 and KATAKRI	
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)

because it merely provides audition criteria. Actually a security guideline for information system development in the state institutions, called "VAHTI 1/2013 Sovelluskehityksen tietoturvaohje" (Software development security guideline), was published separately. This guideline covers security requirements for the information system development. Liitsalo (2013) concluded 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 its controls have been removed from ISO/IEC 27002:2013. At the time ISO/IEC 27002:2005 was published, the electronic commerce was emerging and it was seen as an important domain to cover. As the time passed, also many other information systems became available through the internet. Hence, the electronic commerce turned out as only 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 the case of a security incident. In KATAKRI, one finds very limited requirements to cover such collection of evidence. 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 the reporting of security weaknesses. ISO/IEC 27002 has a specific control (13.1.1 in version 2005 and 16.1.3 in version 2013) to emphasize employee responsibility to report observed or suspected security weaknesses and vulnerabilities. KATAKRI does not contain requirement that would highlight such responsibility, 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 the specifications. Where ISO/IEC 27002 provides implementa-

tion instructions types for compliance and how to achieve the compliance, KATAKRI has only the basic requirement that all operations must be compliant according to the legislation.

5.3. KATAKRI Complements

KATAKRI has some topics that are not part of the ISO/IEC 27002 standard. 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 is to 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 a continuous process. It is notable that there are no requirements for annual security programme at the base level, but they are only 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 objectives or implementation guidance. One such topic was training, where a requirement in KATAKRI defines that the arranged trainings must be documented, including training material and participants. ISO/IEC 27002 controls have similar control to raise the awareness, but implementation guidance does not cover the documentation of training. Similar widely used documentation requirement was in 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 the 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 a competitive advantage, these controls may not be feasible to implement. They don't have high benefit-cost ratio and are only necessary for security critical businesses.

Hence, KATAKRI is a 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 the recruitment. KATAKRI also contains national requirements for physical security alarms. Such requirements are not included in the ISO/IEC 27002 standard.

5.4. 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 the requirements. For example, in some criterions there was, for a certain security level, "No requirements" in English version, but the original Finnish version did contain requirements.

6. RELATED WORK

Jo et al. (2010) concluded a comparative analysis of five ISMSs. The compared methods were Common Criteria, BS7799 (predecessor of ISO/IEC 27001 and 27002), IT Baseline Protection Manual from Germany, ISMS in Japan, and Defense Information Assurance Certification and Accreditation Process (DITSCAP) by the United States Department of Defense (DoD). Analysis was focused on the process, not to the security baseline analysis. An enlarged comparative analysis by the same authors was realized in Jo et al. (2011), where, as a result, a new Information Security Management Evaluation System was proposed.

Beckers et al. (2014) provided a structured method to compare security standards to derive a conceptual model, its template, and a common terminology. The method was applied to three standards; ISO 27001, Common Criteria, and the German IT-Grundschutz standards, resulting into a comprehensive comparison of these standards.

Beckers et al. (2012) linked ISO/IEC 27001 and security requirements engineering (SRE) methods utilizing an existing conceptual framework. Reusing SRE methods supports or-

ganizations to develop, improve, and document their own information security management systems, to be compliant with ISO/IEC 27001 or other standards.

Martins et al. (2013) conducted a case study of applying ISO/IEC 27001 in a military context. In the further research, Martins et al. (2014) proposed a method for the identification of the best combination of security controls to be applied against a particular method of attack. The method takes into account, among other topics, existing security control frameworks, like ISO/IEC 27001, and lessons learned. As the research was conducted in a military context, they also provided support for the military decision making process.

Giacalone et al. (2014) presented a lean approach for the identification of security requirements. The method focuses to overcome the problem of vast amount of resources required to continuously analyze security requirements, when an ISMS is implemented "by the book". The method utilized Security Survey and Triage process to quickly identify the level of relevance of a request for security assessment and the corresponding security requirements. It was recommended to embed such a process as a mandatory step in a company's production cycle.

7. DISCUSSION

In this study, we analyzed ISO/IEC 27002 versions 2005 and 2013 and compared them to the 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 illustrated the evolution of information security management trends (e.g., the role of eBusiness). 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 a number of common security topics that were covered by the both specifications. The results revealed the different scope and lack of some of the controls in KATAKRI compared to ISO/IEC 27001 and ISO/IEC 27002. Moreover, normative controls of KATAKRI were detected, which are not included, even as implementation guidance, in either versions of ISO/IEC 27002.

The structure of KATAKRI makes the evaluation of the organizations' information security management system easier than the one used in ISO/IEC 27002. Where KATAKRI is already structured in the form of the compliance criteria, ISO/IEC 27001 requires more expertise to analyze the appropriateness of the implementation of the security controls to the specific organization. Actually the specifications complement each other well and ISO/IEC 27001 auditor may find KATAKRI as a usable tool to perform the security auditions. One specific difference between the two specifications is the high security level requirements contained in KATAKRI. These can be in the interest of the organizations that need to perceive very high security level in their operations. ISO/IEC 27002 implementation guidance does not contain such level of details that are included in KATAKRI's high security level requirements.

The common security topics are well covered by both specifications and majority of the controls and requirements are found in their intersection. KATAKRI adds more specific requirements on the increased and the high security levels. Organizations having these levels of KATAKRI's security certification should be able to obtain and retain ISO/IEC 27001 certification with little enhancements. From the structural point of view, KATAKRI defines more requirements to be fulfilled and, therefore, an organization may be required to fulfill additional requirements to those that has been acceptable in the ISO/IEC 27001 certification.

KATAKRI is an example of a national approach that it is not initially build as ISO/IEC 27001 compliant. On the other hand, German national BSI IT-Grundschutz has been developed to provide ISO/IEC 27001 compliance.

Martins et al. (2014) used ISO/IEC 27001 in a military context, which was also the background of KATAKRI. Based on our analysis of the contents of these specifications, quantum of complements to ISO/IEC 27001 is not significant. Hence, KATAKRI could be modified to be ISO/IEC 27001 compliant with minor additions.

It has been noticed that SMEs have to focus more on the development of their information security procedures, but most of the ISMS standards are not usable from an SME organization point of view. While SMEs struggle with limited resources, but increased threads, it is important to develop new approaches that are especially suitable for SMEs. Majority of modern information security management systems, including ISO/IEC 27001, are developed for at least medium sized enterprises. One solution could be to provide methods with prioritization of controls to support, at least, a basic selection of potential roadmaps for smaller enterprises. KATAKRI contains basic prioritization using classification levels and recommendations for the industry while ISO/IEC 27002 states in its documentation that security controls are not in any means prioritized. Even at the lowest security level of KATAKRI, amount of controls is out reach for SMEs where security is not a 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. Our research continues to develop methods for SMEs to enhance their security management in a cost-effective fashion.

REFERENCES

Armstrong, C. J. (2013). An approach to visualising information security knowledge. In R. C. Dodge Jr & L. Futcher (Eds.), *Information assurance and security education and training* (pp. 148–155). Springer Berlin Heidelberg. doi:10.1007/978-3-642-39377-8_16

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*, 308-308. doi:10.1109/HICSS.2008.167

Beckers, K., Côté, I., Fenz, S., Hatebur, D., & Heisel, M. (2014). A structured comparison of security standards. In M. Heisel, W. Joosen, J. Lopez & F. Martinelli (Eds.), Engineering secure future internet services and systems (pp. 1-34) Springer International Publishing.

Beckers, K., Faßbender, S., Heisel, M., Küster, J., & Schmidt, H. (2012). Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. In G. Barthe, B. Livshits, & R. Scandariato (Eds.), *Engineering secure software and systems* (pp. 14–21). Springer Berlin Heidelberg. doi:10.1007/978-3-642-28166-2_2

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*.

Giacalone, M., Mammoliti, R., Massacci, F., Paci, F., Perugino, R., & Selli, C. (2014). Security triage: A report of a lean security requirements methodology for cost-effective security analysis. *IEEE Fourth International Workshop on Empirical Requirements Engineering (EmpiRE) 2014*, 25-27. doi:10.1109/EmpiRE.2014.6890112

ISO. (2004). [*Conformity assessment — vocabulary and general principles*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *17000*, 2004.

ISO. (2005). [*Information technology – security techniques – information security management systems – requirements*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27001*, 2005.

ISO. (2005). [*Information technology – security techniques – information security management systems – code of practice for information security management*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27002*, 2005.

ISO. (2011). [*Conformity assessment - requirements for bodies providing audit and certification of management systems*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *17021*, 2011.

ISO. (2011). [*Information technology — security techniques — requirements for bodies providing audit and certification of information security management systems*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27006*, 2011.

ISO. (2013). [*Information technology – security techniques – information security management systems – requirements*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27001*, 2013.

ISO. (2013). [*Information technology – security techniques – information security management systems – code of practice for information security management*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27002*, 2013.

ISO. (2014). [*Information technology — security techniques — information security management systems — overview and vocabulary*. Geneva, Switzerland: ISO copyright office.]. *IEC*, *27000*, 2014.

ISO 19011:2011. (2011). *Guidelines for auditing management systems*. Geneva, Switzerland: ISO copyright office.

ISO 55000:2014. (2014). *Asset management — overview, principles and terminology*. Geneva, Switzerland: ISO copyright office.

ISO/Guide 73:2009. (2009). *Risk management — vocabulary*. Geneva, Switzerland: ISO copyright office.

Jo, H., Kim, S., & Won, D. (2010). A study on comparative analysis of the information security management systems. In D. Taniar, O. Gervasi, B. Murgante, E. Pardede, & B. Apduhan (Eds.), *Computational science and its applications – ICCSA 2010* (pp. 510–519). Springer Berlin Heidelberg. doi:10.1007/978-3-642-12189-0_44

Jo, H., Kim, S., & Won, D. (2011). Advanced information security management evaluation system. KSII. *Transactions on Internet and Information Systems (Seoul)*, *5*(6), 1192–1213. doi:10.3837/tiis.2011.06.006

KATAKRI. (2011). *National security auditing criteria version II*. Finland: Ministry of Defence.

Liitsalo, L. (2013). *Tietoturvallisuusvaatimukset puolustusvoimien tietohallintopäätösmenettelyn mukaisessa tietojärjestelmähankkeessa*. Helsinki, Finland: Aalto University.

Martins, J., dos Santos, H., Dias, M., & Borges, J. (2014). Planning method of information security for military organizations. *Proceedings of the 13th European Conference on Cyber Warfare and Security*, 140-149.

Martins, J., dos Santos, H., Rosinha, A., & Agostinho, V. (2013). Information security management: A case study in a portuguese military organization. [IJCWT]. *International Journal of Cyber Warfare & Terrorism*, *3*(3), 32–48. doi:10.4018/ijcwt.2013070103

NIST Special Publication 800-53. (2009). *Recommended security controls for federal information systems and organizations* (Revision 3). 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*, *34*(1), 48–59. doi:10.1016/j.csi.2011.05.005

Ramanauskaite, S., Olifer, D., Goranin, N., & Cenys, A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications & Control*, *8*(6), 878–890. doi:10.15837/ijccc.2013.6.764

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100. doi:10.1145/1145287.1145316

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. doi:10.1016/j.im.2008.12.007

Weiss, S. (2008). Industrial approaches and standards for security assessment. In I. Eusgeld, F. Freiling, & R. Reussner (Eds.), *Dependability metrics* (pp. 166–175). Springer Berlin Heidelberg. doi:10.1007/978-3-540-68947-8_14

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*, *31*(4), 360–365. doi:10.1016/j.ijinfomgt.2010.10.006

APPENDIX

Table 5. 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

CALL FOR ARTICLES

International Journal of Cyber Warfare and Terrorism

An official publication of the Information Resources Management Association

MISSION:

The mission of the **International Journal of Cyber Warfare and Terrorism (IJCWT)** is to explore a range of security related topics and generate research debates in relation to cyber warfare and terrorism. Targeting researchers, practitioners, academicians, government officials, military professionals and other industry professionals, IJCWT provides a forum to discuss human, technical, and policy issues in relation to cyber warfare and terrorism.

ISSN 1947-3435
eISSN1947-3443
Published quarterly

COVERAGE/MAJOR TOPICS:

- Censorship
- Crisis response and management
- Critical infrastructure protection
- Cyber Terrorism
- Cyber Warfare
- Electronic civil disobedience
- Ethical, political, legal, and social issues relating to security
- Governance and security
- Hacking
- Hacktivism
- Homeland security
- Impact of new security technologies
- Information Management
- Information Security
- Internet and controls
- Law Enforcement
- Manipulation
- National identification schemes
- National security
- Privacy
- Protecting society
- Rights of the individual
- Social engineering
- Terrorism

All inquiries regarding IJCWT should be directed to the attention of:
Graeme Pye, Editor-in-Chief
graeme.pye@deakin.edu.au
All manuscript submissions to IJCWT should be sent through the online submission system:
http://www.igi-global.com/authorseditors/titlesubmission/newproject.aspx

Ideas for Special Theme Issues may be submitted to the Editor-in-Chief.

Please recommend this publication to your librarian. For a convenient easy-to-use library recommendation form, please visit:
http://www.igi-global.com/IJCWT