Utilization of the Finnish National Security Auditing Criteria "KATAKRI" in the EU FP7 PERSEUS project

Jyri Rajamäki

***Abstract*—**Protection of European borders and Seas through the Intelligent Use of Surveillance (PERSEUS) is an FP7 demonstration project supported by the FP7 Security Research theme under DG-Enterprise. Its purpose is to build and demonstrate an EU maritime surveillance system integrating existing national and communitarian installations and enhancing them with innovative technologies. When connecting together surveillance systems of two or more organizations, the trust for others and their cyber security is the main issue. Security audit is a way to demonstrate an organization's security level. This multiple case study analysis consists of six individual case studies that research how the Finnish national security auditing criteria KATAKRI is suitable for different types of organizations when they are developing their security levels. The cross-case conclusions investigate, how KATAKRI could be applied when developing information security policies of different organizations in the perspective of information sharing. The results revealed that KATAKRI is a useful tool for developing organizations' security policies. However, KATAKRI should be redeveloped towards a tool that encourages and simplifies information sharing instead of being a burden.

***Keywords*—**information security management system, information security policy, KATAKRI, multiple-case study, PERSEUS, Seventh Framework Programme.

I. Introduction

FAST adaptation of social media and new mobile phones based on new unprotected technology has increased cybercrimes. The introduction of multiple ICT devices in organizations has made them more vulnerable towards sophisticated and targeted attacks and cyber security is now threatened not only regarding single sources of information, but also regarding the knowledge that derives from the combination of information from multiple sources [1]. However, the ideal of limiting the privacy of individual users in cyberspace to ensure better information security is not acceptable anymore [2]. Governments can retain their mandate to disclose identities, but only if circumstances warrant such breaches of privacy, and any breach of privacy has to be supervised [2].

Social engineering is an increasing threat that Social engineering opens the new possibilities for attacker trough the vulnerabilities of human interaction in cyberspace [3]. Social engineering methods, such as phishing or spear phishing, incorporates sophisticated security attacks which manipulate humans into performing certain actions as authorized users (which they would not do otherwise) or into revealing confidential information [1]. The success of social engineering relies mainly in psychological tricks persuading people to unintentional act against security.

Protection of European borders and Seas through the Intelligent Use of Surveillance (PERSEUS) represents a sample of demonstration research project implemented by the Seventh Framework Programmer (FP7) Security Research Theme. The collaborative research environment of this study involves ISDEFE (Ingeniería de Sistemas para la Defensa de España) in Madrid, Spain (questionnaires) and Laurea University of Applied Sciences in Espoo, Finland. PERSEUS is coordinated by INDRA Sistemas S.A. with 29 international research participators from 12 different EU countries, most of them having maritime frontiers. The purpose of PERSEUS is the protection of the European seas and its frontiers with the intelligent use of technology. One of the project's goal is to develop and test a European system for maritime surveillance through the integration of the European and local systems and its update and improvement using technological innovation [4].

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization's policies and practices for personnel collaboration [5]. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices [1]. Developing of policies that can defeat the main reasons driving non-compliance, such as a habit, is challenging.

KATAKRI is a Finnish national security auditing criteria that is based on several information security management system standards and best practices. This multiple case study analysis consists of five individual cases in different organizations that

This work was supported in part by the European Community's Seventh Framework Programme under the theme Security (FP7-SEC-2010-1).

J. Rajamäki is with Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland (phone: +358-40-7642750; fax: +358-9-88687200; e-mail: jyri.rajamaki@laurea.fi).

research how KATAKRI is suitable for them. The cross-case conclusions examine what type of usability KATAKRI has in information security policy development and implementation in general. The study is carried out according to Yin's case study research (CSR) model [6].

This paper has six sections. The second section briefly introduces the research approach and process. A theoretical framework is presented in the third section where there are an introduction to secure management and governance, secure audits and KATAKRI. The fourth section presents the six empirical cases, from which the results and findings of this paper are based on, units of analysis, and the research data. The fifth section makes cross-case conclusions, and the last section concludes the study and presents future research topics.

II. Research Approach

Figure 1 shows how CSR is applied in this research. The initial step in designing CSR consists of theory development, and the next steps are case selection and definition of specific measures in the design and data collection process. Each individual case study consists of a whole study, and then conclusions of each case are considered to be the replication by other individual cases. Both the individual case and the multiple-result should be the focus of a summary report. For each individual case, the report should indicate how and why a particular result is demonstrated. Across cases, the report should present the extent of replication logic, including certain and contrasting results [6].

Yin notes that the simplest multiple-case design would be the selection of two or more cases that are believed to be literal replications; a more complicated multiple-case design would result from the number and types of theoretical replications [6]. He suggests five to six or more replications for a higher degree of certainty.

The general characteristics of research designs serve as a background for considering four types of specific designs for case study [6]: (1) single-case (single unit of analysis —holistic), (2) single-case (multiple units of analysis — embedded), (3) multiple-case (single unit of analysis —holistic) and (4) multiple-case (multiple units of analysis—embedded). For him, single cases are a common design for doing case studies, especially under certain conditions where the case represents: (1) a critical test of existing theory; (2) a rare or unique circumstance or (3) a representative or typical case, or where the case serves (1) revelatory or (2) longitudinal purposes. He maintains that a single case study should follow sampling logic [6].

In Figure 1, the dashed-line feedback represents a discovery situation, where one of the cases does not suit the original multiple-case study design. Such a discovery implies a need to reconsider the original theoretical propositions. At this point, redesign should take place before proceeding further, and in this view the replication approach represents a way of generalizing that uses a type of test called falsification or refutation, which is the possibility that a theory or hypothesis may be proven wrong or falsified [7].

Doing case study research is a linear but iterative process, and it includes six phases: (1) plan, (2) design, (3) prepare, (4)

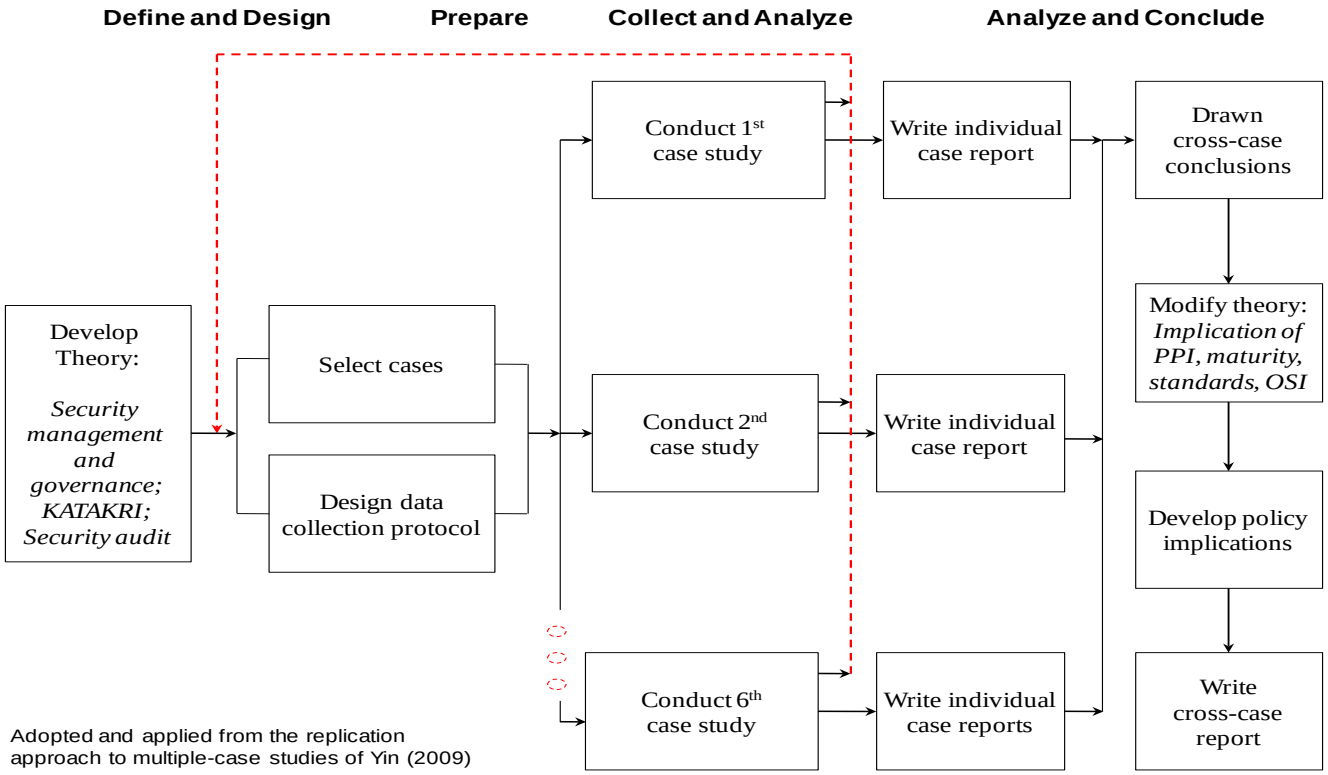

Fig.1 Multiple-case study method of this research

collect, (5) analyze and (6) share [6]. Case studies are the preferred method when: (1) "how" and "why" questions are being posed, (2) the investigator has little control over events and (3) the focus is on a contemporary phenomenon within a real-life context [6]. Phase 1 includes the identification of the research question or other rationale for doing case study, deciding to use the case study method over other methods and understanding its strengths and limitations. The challenge of a case study approach is that there will be many more variables of interest than data points, in which case multiple sources of evidence should be used, with the data needing to converge in a triangulation [8, 9]. Phase 2 includes activities such as defining the unit of analysis and likely case(s) to be studied; developing and articulating theory (e.g., what is being studied and what is to be learnt, propositions and issues underlying the anticipated study); identifying the case study design (e.g., single, multiple, holistic or embedded) and finally defining and designing procedures to maintain the case study quality (e.g., construct validity, internal validity, external validity and reliability) [6]. Phase 3 consists of the skills the investigator should have to conduct a case study and covers the preparation and training for the specific case study, including procedures for protecting human subjects, the development of a case study protocol, the screening of candidate cases that are to be part of case study and conducting a pilot case study [6]. In Phase 4, the case study evidence may come from six sources: documents, archival records, interviews, direct observation, participant-observation, and physical artifacts. Phase 5, consists of examining, categorizing, tabulating, testing or otherwise recombining evidence to draw empirically based conclusions [6, 8]. Every case study should follow a general analytic strategy, whether such a strategy is based on (a) theoretical propositions, (b) case descriptions, (c) using both quantitative and qualitative data or (d) rival explanation. According to Yin (2009), the use of a strategy is necessary for the reduction of potential analytic difficulties and for the definition of priorities as to what to analyze and why [6]. The main analyzing techniques for case studies are: (I) pattern matching, (II) explanation building, (III) time series analysis, (IV) logic models and (V) cross-case synthesis [6]. A persistent challenge is to produce high-quality analyses, which require attending to all the evidence collected, displaying and presenting the evidence separate from any interpretations and considering alternative interpretations [6, 8-12]. Phase 6 consists of reporting the case study, which means bringing its results and findings to closure [6]. Regardless of the form of the report, similar steps underlie the case study composition: identifying the audience for the report, developing its compositional structure, and having drafts reviewed by others [8, 12, 13].

III. Theoretical Framework

As the theoretical foundation of this study, we look security management and governance systems, security audit processes and the Finnish National Security Auditing Criteria, KATAKRI.

A. Security Management and Governance

Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization's information assets that do preserve [14]. ISMS provides controls to protect organizations' most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that security of organization is properly managed and meets regulatory security requirements [15]. An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before business relationship is established. Unfortunately, ISMS standards are not perfect 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 [16].

B. Security Audit

Many different types of audits exist, including financial audits, property assessments, supplier reviews, contractor evaluations, registration audits, equipment evaluations [17], etc. Fig. 2 illustrates internal (first-party) and external (second-party and third-party) auditing types. The common principle is that they compare applied procedures, as well as a set of collected information, against some established criteria.

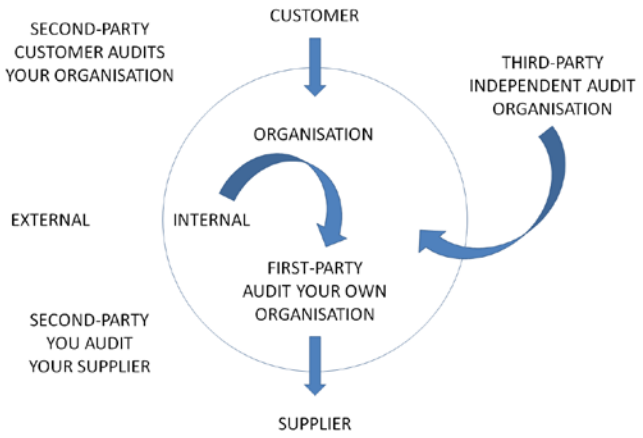

Fig. First-, second- and third-party audits (adapted from [18])

ISO/IEC 17021-2 is a normative standard intended for use by accreditation bodies when assessing management systems, while ISO 19011 provides guidelines for first-, second- and third-party auditors when auditing management systems. The third-party certification industry will use ISO 17021-2 to define requirements for audits and audit arrangements and accreditation bodies will determine whether a certification body's auditing arrangements and activities comply with those

requirements. ISO 19011 identifies best practice and provides information on what should be done when carrying out an audit without specifying how it must be done. ISO 19011:2011 edition includes an extension of the standard's earlier scope of application from quality and environmental management systems to all types of management systems auditing. Continuing development of management systems standards for information security, for example, means that ISO 19011 must be able to accommodate differing requirements while still providing useful guidance [19].

The three things that make a management system audit different from other types of assessments are that the audit must be (1) systematic, (2) independent and (3) documented. In order to conduct systematic management system audits, there is a need for both audit procedures and an audit programme. From an independence point of view, auditors cannot audit their own work or that of their colleagues', as there would be a conflict of interest. Audits need to be structured, to ensure they are free from bias and conflicts of interest. Audits must be documented, because they are all about making decisions and taking action [17].

C. KATAKRI

The root of the Finnish National Security Auditing Criteria, KATAKRI, is to preserve the confidentiality of any confidential and classified information held by the organization concerned. It is published by the Ministry of Defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority (FICORA), Ministry of Foreign Affairs and Ministry of the Interior have also participated in the preparation of the criteria. KATAKRI was officially published in November 2009, and the first update was published in mid-2011 [20]. Version III is currently under revision.

The National Security Auditing Criteria are mutual security criteria for officials and companies for unifying the communal security procedures and to improve self-monitoring and auditing. The National Security Auditing Criteria are an auditing tool used by the officials when carrying out inspections on the level of security within a company or a community. According to the current version of the criteria, KATAKRI's main goal is to harmonize official measures when an authority conducts an audit in a company or in another organization to verify their security level. The National Security Authority (NSA) uses KATAKRI as its primary tool when checking the fulfilment of security requirements. The preface to the criteria states that the second important goal is to support companies and other organizations, as well as authorities and their service providers and subcontractors, in working on their own internal security. For that reason, the criteria contain recommendations for the industry that are separate and outside of the official requirements; it is hoped that useful security practices will be chosen and applied, thus progressing to the level of official requirements.

Criteria are divided into four main areas: (1) administrative security, (2) personnel security, (3) physical security, and (4) 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.

The Web page 'Ministry of Defence of Finland – National Security Auditing criteria (KATAKRI)' relates: 'KATAKRI-criteria have been created from the perspective of absolute requirements and they do not include a marking system which is used in some criteria. The aim here is to make sure that at the end of an audit there would not be possibly unidentified but critical risks. The chosen approach means specific demands for the personnel conducting security audits and, as a result, high enough training level requirements are set to satisfy these demands.'

IV. Empirical Cases

This section briefly describes the five empirical cases that belong to this multiple case study analysis. The individual case report were published earlier; three of them in the shape of bachelor's thesis, one as a master's thesis and one as a conference paper.

A. Case I: Finnish Authority Unit

The individual study report (bachelor's thesis [21]) is available in Finnish. The main objective of this study was to authenticate the security management level in the Finnish authority unit. Authentication was performed using KATAKRI. The other objective was to examine what type of usability KATAKRI has in such an authority unit. This was not an official audit according to KATAKRI, even if the verification was adapted from the actual security audit process. Security assessment was also limited only to the administrative security, in other words security management and its requirements for the increased level (III).

This case study was a qualitative research project, the research methods of which were document analysis, interviews and observation. The hermeneutical method was used as the qualitative research genre. The primary data collection method was the review of security documents, the second method was structured interviews with questions based on KATAKRI and the third method was observation, in practice monitoring the security management activities of the target unit.

The results were drawn up on the result analysis that formed the basis for a summary of developments to the security management. If necessary, these developments can be used by the object to improve their level of requirements and administrative security or to form a development plan for security.

As a result of this case study, a comprehensive, security-perspective report on security management about the unit was obtained. Importing KATAKRI to the authorities' environment seemed to be highly challenging at first. However, time by time the organization learned how to apply observations to the requirement levels of KATAKRI and to the operating environment. KATAKRI as a tool was not already familiar to the unit. However, low awareness could create some authenticity to processes of interviews and observations. If the audit should be carried out exclusively with documentation and its information, would authentication of requirement levels would be inadequate.

This security audit formed as a pre-audit for the unit. If the unit carried out the official KATAKRI audit process, the pre-audit report given to the unit could help to prepare for it considerably better. Based on the result analysis of the pre-audit report it can be stated that the security management level of the authority unit could not reach the requirements of the increased level (III) of KATAKRI on administrative security. However, the object reached the maximum level of requirements of the base level.

B. Case II: Four Private Companies

The individual study report (master's thesis [5]) is available in Finnish. Security within entrepreneurship is an essential factor in the preservation and growth of Finland's international competitiveness. In order to achieve its strategic goals, a company must guarantee the security of its people, its reputation, information, assets and environment. The creation of a company's security policy is the starting point for goal-directed and systematic security management.

The aim of this case was to outline the drafting process of a security policy and the best procedures for defining its content. An additional aim was to formulate a model for a company's security policy and to provide recommendations for its implementation. The basis for the empirical case study was formed by interviews carried out in four companies. The interview framework used the National Security Auditing Criteria KATAKRI.

The results of the work revealed that companies have deemed the security policy useful, since all companies had already composed their own security policy (or a similar document). On the other hand, the individual contents and practices of the different security policies differed quite a lot from each other. There was a lack of a common operation model, so this case study aims to even out discrepancies in the future. In particular, the companies found particularly the implementation of security policies within their organizations to be a challenge.

After the case study research, a model for a company's security policy was created. It is meant to be freely utilized by all Finnish companies and organizations.

C. Case III: An Adult Education Centre

The individual study report (bachelor's thesis [22]) is available in Finnish. This case study research focused on how an adult education centre can prepare internally for a security auditing process. The purpose of this case was to achieve administrative security control by internal audit. Internal audit was based on KATAKRI and it was executed in an authentic learning institution environment. The need for this study was practical: research results serve security management in general and offer one tool to control security issues in the school environment.

First, the study researched the prevailing and the ideal security situation of the adult education centre. The target level was set at the recommended level of KATAKRI administrative security because it meets best the needs of the examined education centre. The research methods used were observation and literature overview. After the case study research, a model of an internal auditing process in an adult education centre was described. The model was presented from a continuing development point of view, utilizing the Deming PDCA (plan-do-check-act) cycle model.

Security matters of different learning institutes have recently had a great deal of media coverage. The results of this case show that education centres are ready to work for a better security level. However, problems occur due to lack of time resources, explicit tools or adequately defined goals. These weaknesses have a negative impact on the development of security culture.

D. Case IV: Company X's Personnel Security and Physical Security

The individual study report (bachelor's thesis [23]) is available in Finnish. The purpose of this case study was to execute a pre-audit to Company X in the fields of personnel security and physical security. The pre-audit was based only on KATAKRI. The study was executed from a consultant's perspective and with the principles of a functional case. The objectives of the study were to compare the state of Company X's personnel security and physical security fields with KATAKRI's demands. The study was defined to cover only the personnel security and physical security sections of KATAKRI. For both of the audited security fields, were chosen their own objective levels of KATAKRI. One of the objectives of the study was also to evaluate the compatibility and usefulness of KATAKRI compared to the needs of Company X. One of the reasons for evaluating it was to examine possible benefits that the company might receive from an official KATAKRI audit.

In addition one of the purposes of the study was to develop steps to improve the deficiencies found based on the audit. The study itself consists of four main categories: context, theory basis, execution of the study and conclusions. The context depicts the operational environment, theme, execution stages and definitions of the study. The theory basis forms a scientific based information basis to the study and the execution study describes the audit process and its results.

The conclusions category consists of the evaluations of the audit results and the improvement steps. The objective of the study was to produce results from two different perspectives: evaluating the compatibility and usefulness of KATAKRI and the fulfilling of the KATAKRI's audit requirements. The results of the audit were relatively good. Almost all the requirements were met by both the personnel and physical security sections and the identified deficiencies were only minor. The biggest challenges with the results concerned the compatibility of KATAKRI. The challenges were mainly affiliated with some obscurities and interpretational challenges. There were also many audit requirements that were not suitable for Company X. The main challenge occurred to be the question, whether a whole security section of KATAKRI can be approved in an audit even though all of the requirements of the audit questions in that particular section are not met.

As for the conclusions, it can be noted that the study was in its entirety useful for Company X. The company gained a fair view of the level of its audited operations and objects compared

to the requirements of KATAKRI. Most of all the company gained knowledge and understanding of KATAKRI's compatibility for the company's requirements. With the study Company X is able to weigh the pros and cons of a real official KATAKRI standardization audit and to evaluate its usefulness for the company itself.

E. Case V: Expectations for Security Auditing Criteria, Processes and Auditors

The individual study report [24] is available. The object of the case study was to give understanding and background information for improving security audits. The case study was conducted in the form of interviews, questionnaires and observations. In the first phase, nine highly experienced experts in the fields of security and safety were interviewed. They were selected according to their experience and organizations: four of them represented authorities, three represented private companies, one was a researcher and one was a consultant. The interviews lasted 1 to 2.5 hours each and were recorded, transcribed and analyzed with the ATLAS.ti computer program. Two different Webropol questionnaires (N=31, N=14) were circulated to graduate security management and ICT students at a Finnish higher education institute. The aim was to find out whether students, academia and professionals would be interested in security auditing studies and what are their opinions on the content of such studies.

The first KATAKRI leading auditor training course was executed between Feb 2012 and Dec 2012. The case study evidences included observations and lessons learnt from the course. Also, 16 expert interviews were carried out within the course, three of the interviewees represented authorities, ten represented security auditing companies and three were researchers. Multiple types of documentary information (memoranda, written reports of events, progress reports, course material, dissertations and other study reports, newspaper and magazine clippings, etc.) were used to corroborate and augment evidences from other sources.

The main result of the study was that KATAKRI audits have different objectives depending upon the reason for the auditing process being executed. The audit team leader must be aware of these objectives and act according to them. However, the most important tool for auditors to carry out their work is a functioning governance system. This means that auditors should invest in improving criteria so that they are reasonable, topical and functional. In practice, this means that auditors should analyze audit findings as well as monitor KATAKRI's requirements and auditing processes. When needed, they should participate in KATAKRI renewals and develop auditing processes.

F. Case VI: Developing an Information Security Management System

The individual study report (bachelor's thesis [25]) is available. The purpose of this case study was to study development of an information security management system and study the resources and components, which combined create a functional information security management system. To reach the target objective, the case first examines the international and international legislation regarding information security. Secondly, the information security related international and national standards and frameworks are analyzed and compared. Finally the outcome of case is presented as a reflection of previously studied components of information security management systems.

This case was carried out as a basic research to expand the knowledge of the phenomena and develop current practices. Literature overview was used as the research method, as it is the most eligible method to explore the aims of this study. Literature overview was selected to collect in-depth data of the phenomena.

This case sought to answer the question of what are the components of an effective information security management system. The first part of the case process opened this from the perspective of international and national laws and regulations. Second part focused on international and national standards and frameworks that can be utilized to create effective information security management systems.

During the case, it came clear that Finland does not have a uniformed information security legislation that could be followed to guide to process of creating information security management system. The newly released national implementation program of the cyber security strategy clarifies the responsibilities of national information security by assigning roles to various actors. It does not, however, provide support for those not working in the critical infrastructure, and therefore effectively leaving out great number of Finnish organizations. The cyber security strategy is a great start to improve the national information security, but is not enough alone. Therefore, the first suggestion of this thesis is for national actors to unify the legislation related to cyber and information security, and therefore making it more accessible to a wider audience.

Currently there are multiple international information security standards, which organizations can choose to adopt into their own processes. On a national level the VAHTI instructions and KATAKRI provide good start for the standardization process for small and medium size organization. However, these standards are created for a narrow special purpose and are not applicable to all situations. International standards can be with some effort modified to support the needs of Finnish organizations. The second suggestion of this thesis is to start developing a national standard for information security, which can be used as a guideline in creating an information security management system for any size organization and which is specified for the needs of Finnish organizations.

During the case, it came clear that information security management systems can be applied to an organization of any size, but they easily grow to be too large to be effectively managed and follow. Therefore, it is critical for companies to carefully plan the information security management system, before starting to adopt it to cover all the processes of the organization. Most important requirement for all these systems is the support from the upper-management and employees who

are part of that system. The support must be visible and continuous in order for the system to stay functional.

V. Cross-case Conclusions

When developing an organization's security policy, KATAKRI criteria are a good basis for structural interviews of stakeholders, because the criteria look comprehensive security from four areas: administrative security, personnel security, physical security and information security. KATAKRI sets common criteria for all kind of organizations, such as large private companies, small and medium-size enterprises (SMEs), security organizations, and governmental agencies. This brings out challenges with regard to its usability and utility because every criterion is not suitable for every organization.

KATAKRI also has some shortcomings. For example, it has no glossary about the terminology that is used. Each question contains the requirements to all security levels and 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. However, the lack of the common ontology can be seen as a major weakness of KATAKRI that leaves possibility for interpretation instead of having exact requirements for ISMS.

The results of our cross-case analysis revealed that companies have deemed the security policy useful, since all companies had already composed their own security policy (or a similar document). The development of the security policy requires understanding of people's decision-making processes concerning ICT use. In some organizations, clear objectives of the security policy are missing and, as a consequence, its implementation is fragmented. Large organizations usually have dedicated personnel for information security, many security-related areas are under direct control, and there is a vast body of research in that domain. On the other hand, SMEs increasingly have their infrastructures outsourced (or hybrid) and have no internal capacity and expertise for information security management.

According to our cross-case analysis, security policies should define at least the following aspects:

- Long-range goals of security actions
- Short-range aims
- Indicators of long-range goals and short-range aims
- Roles and responsibilities.

According to our multiple case study analysis, most organizations found that the implementation of security policies within their organizations to be a challenge A current trend for easing the implementation of the security policy is that the security policy document is strived to boil down to one page. However, separate training materials are needed and they should go through in different forums, such as the industrial safety commission.

Findings within our multiple case study analysis stands by ideas presented in DIGILE's Strategic research agenda for cyber trust [1]. Further research and development work is needed towards:

- New methods and tools to develop and implement information security policies that can support the continuously changing ICT environments,
- Understanding of the various incentives driving information security investments and change of the mentality from 'security as a burden' to 'security as increasing productivity/performance',
- New resiliency frameworks and processes to increase the integration between business continuity and IT recovery,
- Refinement of risk assessment methods to manage emerging risks,
- Methods, processes and tools to improve information security culture amongst all organizations.

VI. Conclusions

PERSEUS is an FP7 demonstration project supported by the FP7 Security Research theme under DG-Enterprise. Its purpose is to build and demonstrate an EU maritime surveillance system integrating existing national and communitarian installations and enhancing them with innovative technologies. It is a fact that public protection and disaster relief (PPDR) agencies' present-day digital systems do not support cross-border cooperation. In addition to technical challenges, the distrust between agencies (especially in the field of law enforcement and crime investigation) causes trouble. Unfortunately, this distrust also exists at the national level, and even between units of one organization. However, common digital systems and operational procedures could increase the trust between parties. The European Network of Law Enforcement Technology Services (ENLETS) was established as a sub-group of the Law Enforcement Working Party of the EU Council in 2008. ENLETS' vision is to be the leading European platform that strengthens police cooperation and bridges the gap between the users and providers of law enforcement technology. The core group members of ENLETS (The Netherlands, The United Kingdom, Finland, Belgium, Poland and the prevailing EU's presidency country) should develop common procedures to apply new law enforcement technology. In the future, these procedures could be extended to other European countries as well as other field of PPDR.

As Ahokangas et al. [1] says, a very important change is needed, where the mental-picture of cyber security should be changed from "threat, crime, attack" into "trust". In Finland, KATAKRI should be redeveloped towards a tool that encourages and simplifies sharing of mission critical data between PPDR actors.

References

[1] M. Ahokangas, V. Arkko, T. Aura, P. Erkinheimo, A. Evesti, T. Frantti, J. Hautamäki, M. Helenius, M. Hämäläinen, J. Kemppainen, A. Kirichencko, M. Korkiakoski, P. Kuosmanen, M. Laaksonen, M. Lehto, J. Manner, J. Remes, J. Röning, B. Sahlin, R. Savola, V. Seppänen, M. Sihvonen, A. Tsochou and P. Vepsäläinen, "Strategic research agenda for cyber trust," DIGILE, 2014.

[2] I. Bernik, "Information Warfare Effects on Businesses in Slovenia," *Recent Advances in Information Science*, pp. 42-47, 2013.

[3] V. Sobeslav, "Computer networking and sociotechnical threats," *Recent Researches in Circuits, Systems, Communications and Computers*, pp. 105-109, 2011.

[4] R. Pirinen, E. Sivlén and E. Mantere, "Samples of Externally Funded Research and Development Projects in Higher Education: Case

Integration Readiness Levels," P*roceedings of 2014 International Conference on Interactive Collaborative Learning (ICL)*, 2014.
[5] O. Laitinen, "Yrityksen turvallisuuspolitiikan laatiminen," Laurea-ammattikorkeakoulu, Theseus, 2013.
[6] R. K. Yin, *Case Study Research Design and Methods.* Thousand Oaks: Sage Publications, 2009.
[7] K. Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge*. London: Routledge Classics, 2009.
[8] R. Stake, *The Art of Case Study Research.* Thousand Oaks: Sage Publications, 1995.
[9] C. Robson, *Real World Research*. Oxford: Blackwell Publishing, 2002.
[10] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks: Sage Publications, 1994.
[11] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Saga Publications, 2008.
[12] G. Walsham, "Doing interpretive research," *European Journal of Information Systems*, vol. 15, pp. 320-330, 2006.
[13] L. F. Locke, W. W. Spirduso and S. J. Silverman, *Proposals that Work: A Guide for Planning Dissertations and Grand Proposals*. Thousand Oaks: Sage Publications, 2007.
[14] W. Lee and S. Jang, "A study on information security management system model for small and medium enterprises," *Recent Advances in E-Activities, Information Security and Privacy*, pp. 84-87, 2009.
[15] J. S. Broderick, "ISMS, security standards and security regulations," *Information Security Technical Report*, vol. 11, pp. 26-31, 2006.
[16] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, pp. 267-270, 2009.
[17] ISO 19011 Expert [online]. Available: http://www.iso19011expert.com
[18] J. P. Russell, *The ASQ Auditing Handbook*. ASQ Quality Press, 2012.
[19] ISO 19011 vs ISO/IEC 17021-2 - IRCA – Home. [online]. Available: http://www.irca.org/en-gb/resources/INform/archive/issue27/Features/Building-on-safety21/
[20] Ministry of Defence Finland, "KATAKRI, National Security Auditing Criteria. Version II," 2011.
[21] J. Kojo, "Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla," Theseus, 2013.
[22] M. Martiskainen, "Sisäinen turvallisuusauditointi aikuiskoulutusoppilaitoksessa," Laurea-ammattikorkeakoulu, Theseus, 2012.
[23] M. Kimiläinen, "Yritys X: n henkilöstöturvallisuuden ja fyysisen turvallisuuden esiauditointi Kansallisella turvallisuusauditointikriteeristöllä," Laurea-ammattikorkeakoulu, Theseus, 2011.
[24] J. Rajamäki, "Challenges to a smooth-running data security audits. Case: A Finnish national security auditing criteria KATAKRI," *Proceedings of the 2014 European Intelligence and Security Informatics Conference*, 2014.
[25] M. Karjalainen, Developing an Information Security Management System. Laurea-ammattikorkeakoulu, Theseus, 2014.

Jyri Rajamäki received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively. He received his PhD degree in information technology from University of Jyväskylä in 2014.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea's Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored about 140 scientific publications.

Dr. Rajamäki has been an active actor in the field of electrotechnical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge, national coordinator and scientific supervisor for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM.