National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process

Jyri Rajamäki[1] and Merja Rajamäki[2]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]Finnish Safety and Chemicals Agency (Tukes), Helsinki, Finland
jyri.rajamaki@laurea.fi
merja.rajamaki@tukes.fi

Abstract: The National Security Auditing Criteria, KATAKRI, were published in 2009, revised in 2011, and version III is currently under revision. The root of KATAKRI is to preserve the confidentiality of any confidential and classified information held by the organisation concerned. One of KATAKRI's aims is to combine the actions of authorities when verifying the security level of a company or other corporation by carrying out security auditing. From the enterprise operators' point of view, the focus of security auditing is to eliminate unfair competition and maintain an equal opportunity field for operators. Another of KATAKRI's aims is to improve national security when Finnish Defence Forces or other security authorities apply subcontracting. KATAKRI is also intended to help companies and corporations when they are developing their own security level. The purpose of this case study is to find out: what is expected from the security auditing process and from the leading auditor; what kind of competence the auditor should have; and how the security auditing training and qualification should be developed to correspond with the needs of the security field. The empirical research was conducted in the form of interviews, questionnaires and observations made as a student during the first KATAKRI leading auditor course executed 2/2/2012–12/12/2012. The combined results showed that deep knowledge of the security field and competence to manage overall security is required from security auditors. Furthermore, it was concluded that qualifications for security auditors should be created in accordance with ISO Standard 19011:2011, which provides a very strong competence model. In light of the above, it is recommended that the academic level, content and requirements of future audit and security auditing training should be clearly defined, and the quality of the training should be standardised and certified. The results also indicate that KATAKRI version II still has defects due to its inconsistency. One task of auditing processes should be collecting information about KATAKRI's shortcomings, and they should be systematically analysed. Future leading auditor courses would be suitable scenes to analyse shortcomings and to propose improvements to KATAKRI. KATAKRI should be revised every second or third year.

Keywords: KATAKRI, national security auditing criteria, security auditing, security auditing training

1. Introduction

1.1 The National Security Auditing Criteria, KATAKRI

The root of the National Security Auditing Criteria, KATAKRI, is to preserve the confidentiality of any confidential and classified information held by the organisation concerned. KATAKRI was officially published in November 2009, and the first update (Ministry of Defence, *National Security Auditing Criteria, version II*) was published in mid-2011. Version III is currently under revision; the Internal Security Secretariat has appointed a working group to update KATAKRI by 31/12/2013.

According to the current version of the criteria, KATAKRI's main goal is to harmonise official measures when an authority conducts an audit in a company or in another organisation 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 organisations, 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.

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.'

1.2 Auditing procedure

Many different types of audits exist, including financial audits, property assessments, supplier reviews, contractor evaluations, registration audits, equipment evaluations (ISO 19011 Expert), etc. Figure 1 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.

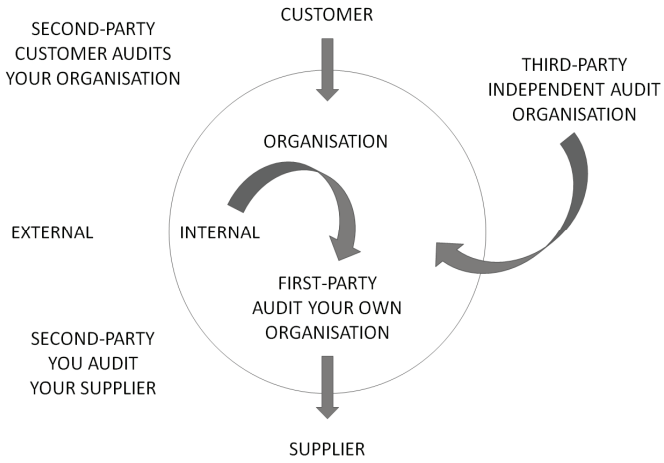

Figure 1: First-, second- and third-party audits (adapted from Russel 2005)

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 (ISO 19011 vs ISO/IEC 17021-2 - IRCA – Home).

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 (ISO 19011 Expert).

1.3 Competence and evaluation of auditors

ISO 19011:2011 includes a section that deals with auditor competence. The section covers determining auditor competence to fulfil the needs of the audit programme, personal behavioural aspects, discipline or sector-specific competence, as well as evaluation and maintenance of competence. In relation to behavioural aspects, auditors should be, for example, open-minded, perceptive, tolerant of pressure, versatile, culturally sensitive and collaborative.

Management system auditors should have generic knowledge and skills needed to audit multiple discipline management systems and implement other parts of ISO 19011:2011. For example, auditors should understand the types of risk associated with auditing. They need knowledge of organisational types, general business and management concepts, processes and related terminology, including budgeting and management of personnel. Auditors should be able to position discipline and sector requirements and audit findings in the wider context of the organisation's business activities, governing agencies, business environment, legal and contractual requirements and management's policies and intentions for the organisation.

Annex A.7 of ISO 19011:2011 describes the knowledge and skills that information security management auditors should have. Auditors who intend to examine information security management systems need to have information security management knowledge and skills. They should be able to apply information security management methods, techniques, processes and practices. They must have the knowledge and skills needed to examine information security management systems and to generate appropriate audit findings and reach valid conclusions.

According to ISO 19011:2011, an audit team leader must have the knowledge and skills 1) to balance the strengths and weaknesses of the individual audit team members, 2) to develop a harmonious working relationship among the audit team members and 3) to manage the uncertainties involved in achieving audit objectives.

1.4 KATAKRI audit team leader training

Due to increasing application of KATAKRI, there is a definite need to teach both the content of KATAKRI and the process of security auditing. Today, many organisations are arranging different kinds of KATAKRI training courses, but the academic level, content and requirements of security auditing training have not yet been defined (Rajamäki 2011). At the initiation of the Ministry of the Interior, Laurea University of Applied Sciences (UAS) organises KATAKRI leading auditor training courses. The first course started in February 2012 and ended in December 2012, and the second started in February 2013. The basic assumption behind any security auditing training course is that the authorities can trust the quality of training and the expertise of those people who have undertaken it.

1.5 Structure of the paper

Section 2 of this paper presents the research targets and methods applied in this study, as well as how the research process has proceeded. In Section 3, the research findings are presented and evaluated against the theories presented in Section 1. Section 4 sets out the conclusions of the study and answers to the research questions. The final section also includes an assessment of the study and suggestions for further research.

2. Research method and process

The purpose of this study is to find out what is expected from the National Security Auditing Criteria, the security auditing process and the audit team leader. We tried to discover what kind of competence the auditor should have and compared these to the suggested competencies of ISO 19011. We analysed KATAKRI's different targets. We also give suggestions regarding how security auditing training and qualification should be developed to correspond with the needs of the security field. This study has been carried out according to the case study method of research represented by Yin (2009). The empirical research was conducted in the form of interviews, questionnaires and observations. Nine highly experienced experts in the fields of security and safety were interviewed. They were selected according to their experience and organisations: 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 analysed with the ATLAS.ti computer program.

Two different Webropol questionnaires (N=31, N=14) were circulated to graduate security management and ICT students at Laurea UAS. The aim was to find out whether students would be interested in security auditing studies and their opinions on the content of such studies.

The first KATAKRI leading auditor training course was executed between 2/2/2012 – 12/12/2012. One of this paper's authors developed the course; another was one of its seventeen participants. This paper provides research results and lessons learnt from the course.

3. Findings and discussion

3.1 Multiple targets of KATAKRI and security audits

As shown in Figure 2, KATAKRI and the security auditing process serve three main clients to: 1) the economic life (companies that develop and sell security products and services), 2) society and 3) companies and other organisations seeking to improve their own internal security.

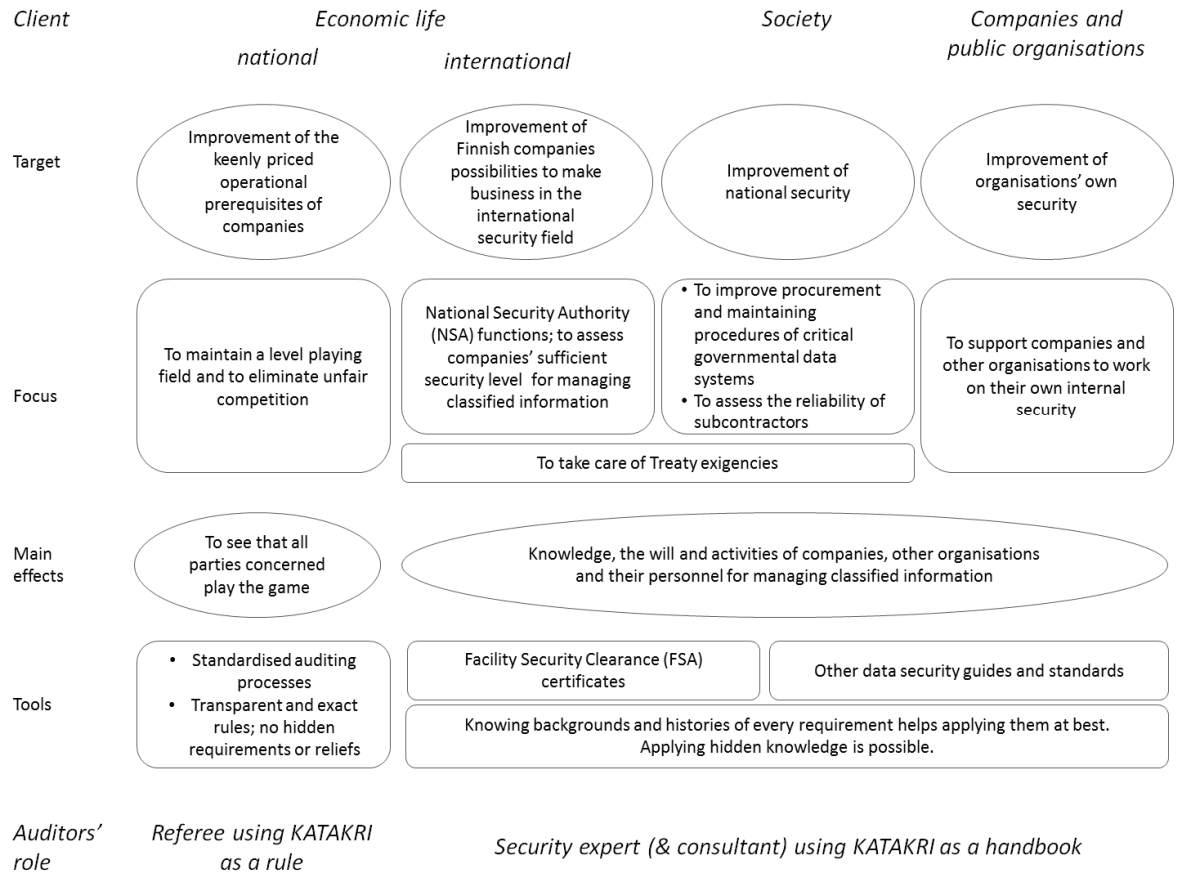

Figure 2: Multiple tasks of KATAKRI audits

From economic life's point of view, the task of security audits could be divided into two parts: a national and an international viewpoint. The national viewpoint is taken into consideration when companies are acting as service providers and subcontractors for Finnish Defence Forces or other national (security) authorities. A normal procedure in these situations is that the new services are put out to tender, and fulfilling KATAKRI's requirements is a mandatory precondition for companies. From this perspective, the main aim of security audits is to eliminate unfair competition and maintain an equal-opportunity market for all companies. To achieve these results, security auditors have to inspect the workings of 'the system' so as to determine that all parties concerned observe their responsibilities. And here, by the 'system', we mean that no organisation will benefit from breaking KATAKRI's requirements on purpose. If an attempt to do this is made, it will be detected, resulting in the organisation fouling its own nest. The role of security auditors is to act as a referee between companies and use KATAKRI as a rule. With regard to this function, auditing processes should be firmly standardised, having transparent and exact rules without any hidden requirements or reliefs.

From international economic life's point of view, the target of security audits is to improve Finnish companies' business opportunities within the international security field. Facility security clearance (FSC) certificates provided by NSA under the terms of bilateral treaties between countries enable Finnish companies to take part of calls for offers with regard to international security critical business. From this perspective, the main aim of security audits is to assess that the company concerned has sufficient security procedures and facilities in place for managing classified information.

From society's point of view, KATAKRI's target is to improve national security. KATAKRI is applied when Finnish Defence Forces or other authorities purchase or subcontract security products or services. From this perspective, KATAKRI's aims are to improve the procurement and maintenance procedures for critical governmental data systems, as well as to assess the reliability of subcontractors. The way to administrate for national security is to attempt to contribute to the knowledge, will and activities of all individuals, companies and other organisations so that security becomes one of the true values which conducts the thinking

behaviour behind their activities. To achieve these results, KATAKRI should be used as a handbook. The role of a security auditor is to act as a security expert and consultant. Knowing the background and target of every requirement helps to best apply these requirements at best. Also, utilising hidden knowledge could improve security.

KATAKRI is also intended to help companies and public organisations developing their own security mechanisms on a voluntary basis. This is why KATAKRI contains recommendations that are separate and outside the official requirements. From this perspective, KATAKRI could be applied as a handbook and security auditors could act as security experts and consultants.

3.2 Multiple roles of KATAKRI auditors

As stated earlier, security auditing involves multiple tasks. This means that security auditors have multiple roles. The two main roles are 1) to referee on the playing field between companies and 2) to act as a security expert and consultant. In most cases, the role of a referee conflicts with the role of a consultant. When auditors are seeking to maintain a level playing field, in principle, they are not able to consult.

In the worst situations, maintaining a level playing field for companies does not improve their security level at all. This is the case if a certain criterion does not actually measure the facility it is meant to. According to Finnish law, security auditors are acting civil servants. So, as shown in Figure 3, with this 'hat' on, the security auditor should also ensure that the governance system is a functional one – here, by the governance system, we mean national legislation, KATAKRI and standardised auditing processes. As a result of this, a very important role for security auditors is continuous monitoring of the security auditing criteria. When needed, security auditors must react and participate in requirement renewals. This includes KATAKRI renewals as well as development of standardised auditing processes. However, because audit findings are confidential information, enforcement of this role is not an undemanding task.

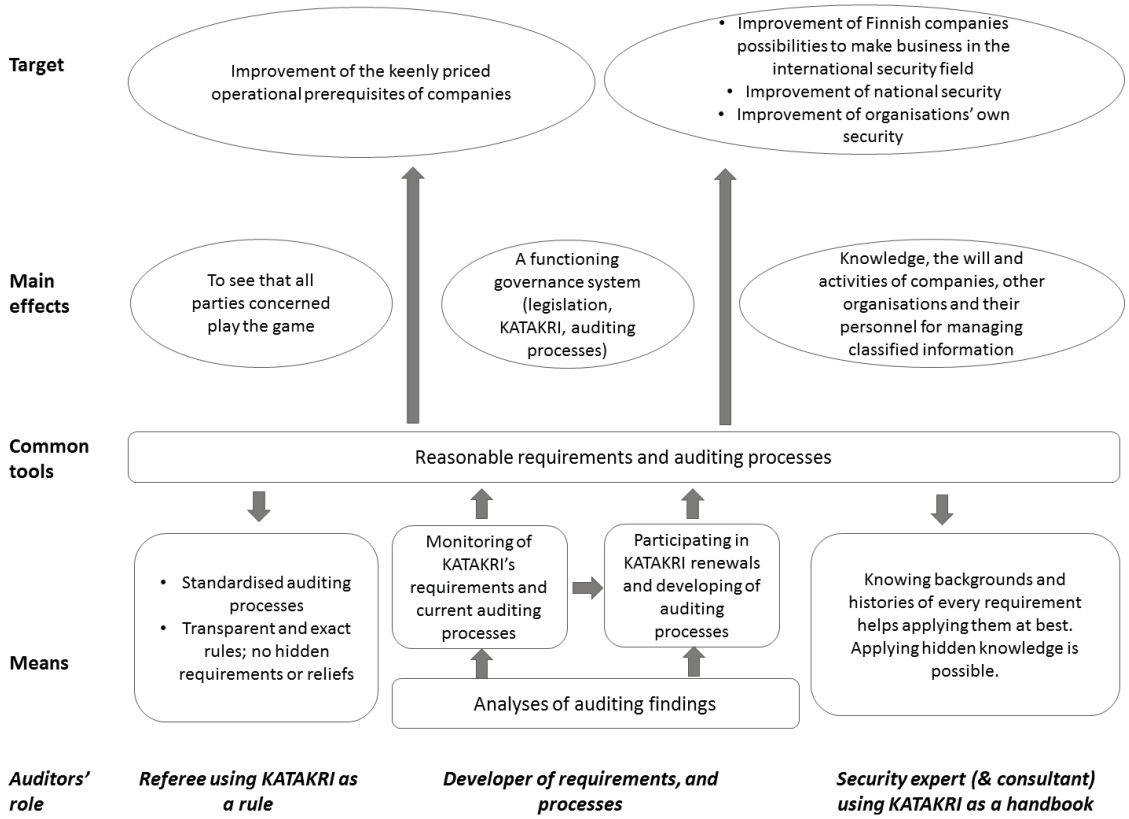

Figure 3: Security auditors' roles, means, tools, effects and targets

3.3 Auditors competences and auditing training

The combined results of the interviews, the questionnaires, and examination of the content of the existing training modules showed that deep knowledge of the security field and the competence to manage the overall security picture is required from security auditors. Furthermore, it was concluded that qualifications for security auditors should be created in accordance with ISO 19011:2011, because it provides a very strong competence model.

In light of the above, it is recommended that the academic level, content and requirements of future audit and security auditing training should be clearly defined, and the quality of the training should be standardised and certified. It would then be possible to plan and implement a different kind of security auditor course for different purposes. For example, the lead auditor course module is a natural module for Laurea UAS to offer to experts from different security branches who want to deepen their know-how regarding leading security audits.

The results also indicate that KATAKRI version II still has defects due to its inconsistency. One task of auditing processes should be collecting information about KATAKRI's shortcomings, and they should be systematically analysed. From the experience of the first leading auditor courses, most participants (students, lecturers) are real security experts with experience of taking part in KATAKRI audits as team members. Future leading auditor courses would be suitable scenes to analyse shortcomings and propose improvements to KATAKRI. KATAKRI should be revised every second or third year.

4. Conclusions

This section evaluates the research process and the findings of this study from the viewpoint of the study's research questions. Finally, suggestions for future research avenues are made.

4.1 Answers to research questions

The main objective of this study was to find out what is expected from KATAKRI, the security auditing process and the leading auditor. As Figure 2 shows, 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 analyse audit findings as well as monitor KATAKRI's requirements and auditing processes. When needed, they should participate in KATAKRI renewals and develop auditing processes.

The new version of ISO 19011 defines quite well the kinds of competence that auditors and the audit team leader should have. It identifies the necessary auditor competence, including generic knowledge and skills of management systems, discipline and sector (e.g. aerospace) knowledge and skills. Informative Annex A gives examples of auditors' discipline-specific knowledge and skills, including e.g. information security. However, no guidance is given regarding auditors' sector-specific knowledge and skills.

Leading auditor courses are forums to disseminate expertise from earlier audits in which the participants have been audit team members. As stated previously, auditors should also monitor the criteria concerned. To put this task into action, every leading auditor course should include a period in which the participants analyse the possible shortcomings and incoherence in KATAKRI. Unfortunately from this perspective, audit findings are confidential information, which limits the possibilities to discuss these issues. Anyway, a suitable academic level for these studies is a graduate school, because the students should have abilities of analysing of findings. These courses could be part of a master's degree in security management or information systems.

4.2 Future research proposal

The security auditing training and qualification should have different steps to correspond with the needs of the security field. Figure 4 offers a rough sketch of 'the ladder' of an individual security expert moving towards becoming the leader of a security audit team. It also outlines the roles of academies (left) and authorities (right), as well as how the organisation concerned could learn within this development process (middle). However, future research is needed to define and design the right steps, their number and their levels. The concrete roles of academies and authorities in achieving each step should also be clarified.

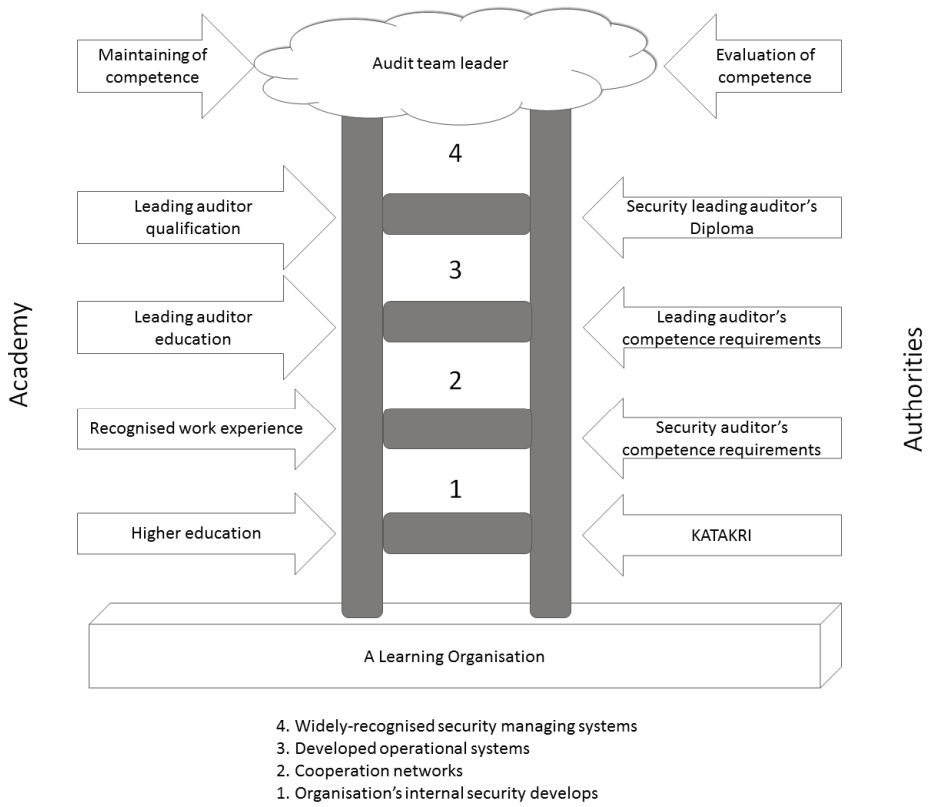

Figure 4: Authorities', organisations', academies' and individuals' contributions and throughputs when applying the competence model of a security auditor

References

ISO 19011 (2011) 'Guidelines for auditing management systems', Geneva: ISO.

ISO 19011 Expert, http://www.iso19011expert.com/ (accessed February 28, 2013).

ISO 19011 vs ISO/IEC 17021-2 - IRCA - Home | International .., http://www.irca.org/en-gb/resources/INform/archive/issue27/Features/Building-on-safety21/ (accessed February 28, 2013).

ISO/IEC TS 17021-2 (2012) 'Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 2: Competence requirements for auditing and certification of environmental management systems', Geneva: ISO.

Ministry of Defence (2011) *National Security Auditing Criteria (KATAKRI),* version II, 2011. http://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf

Ministry of Defence of Finland – National Security Auditing criteria (KATAKRI). [Online], http://www.defmin.fi/en/administrative_branch/defence_security/national_security_auditing_criteria_(katakri) (accessed February 26, 2013).

Rajamäki, M. (2011) *Pätevyysmalli turva-auditoijan tutkintokoulutukselle – tapaustutkimus Laurean Auditoinnin johtaminen –opintojaksosta (Developing a competence model for security auditor specialization studies – Case study: Laurea's Management of Auditing study module).* Master's thesis. Theseus. Espoo: Laurea (in Finnish).

Russel, J. (ed.) (2005) *The ASQ Auditing Handbook*, Milwaukee: ASQ, Quality Press.

Yin, R. K. (2009) *Case Study Research: Design and Methods*, 4th ed., California: SAGE Publications.