Please quote as: Sunyaev, A.; Tremmel, F.; Mauro, C.; Leimeister, J. M. & Krcmar, H. (2009): A Re-Classification of IS security analysis approaches. In: Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS), San Francisco, USA.

Americas Conference on Information Systems (AMCIS)

AMCIS 2009 Proceedings

Association for Information Systems *Year* 2009

A Reclassification of IS Security Analysis Approaches

Ali Sunyaev* Florian Tremmel† Christian Mauro‡
Jan Marco Leimeister** Helmut Krcmar††

*Technische Universitat Munchen, sunyaev@in.tum.de
†Technische Universitat Munchen, florian.tremmel@accenture.com
‡Technische Universitat Munchen, mauro@in.tum.de
**Universitat Kassel, leimeister@uni-kassel.de
††Technische Universität München,, krcmar@in.tum.de

A Re-Classification of IS Security Analysis Approaches

Ali Sunyaev
Technische Universität München, Germany
sunyaev@in.tum.de

Florian Tremmel
Technische Universität München, Germany
florian.tremmel@accenture.com

Christian Mauro
Technische Universität München, Germany
mauro@in.tum.de

Jan Marco Leimeister
Universität Kassel, Germany
leimeister@uni-kassel.de

Helmut Krcmar
Technische Universität München, Germany
krcmar@in.tum.de

ABSTRACT

The role of security management in the development and operation of information systems has a long tradition of research in computer science, information systems and management science. Integrating the economic, organizational, and technical aspects of information systems security analysis and assessment requires a bridging of these different research streams.

We examined major articles published concerning IS security using a new classification scheme for IS security analysis and assessment approaches. We looked at approaches discussed in recent publications as well those examined as in past articles that have attempted to classify various approaches to IS security. This paper therefore organizes a diverse collection of literature into a cohesive whole with the aim of providing IS management with an overview of current security analysis approaches, thereby offering management an effective aide for selecting the methods best suited to their needs. Furthermore, this work structures IS security research into a classification scheme that can also be used in future research and practice.

Keywords

Information Systems Security, Security Management, Risk Management, Information Security Management Standards.

INTRODUCTION

The goal of information systems (IS) security analysis and security assessment is the identification and evaluation of possible threats (Siponen, 2005a): security analysis and security assessment are both integral parts of security management. Various reviews or summaries of information systems security analysis approaches exist, however their respective motivations, backgrounds, and foci differ (Cody, Sharman, Rao and Upadhyaya, 2008). The goal of this paper is to provide an integrated classification of IS security analysis and assessment approaches as a guide to the subject for managers. Unlike previous reviews, we have summarized existing approaches and assigned them into unique and clear categories that were identified during our literature review process. In addition, synonyms and homonyms that appear in the various approaches are identified and classified which allows for better understanding and comparison of the approaches. Furthermore, in contrast to other works, this paper does not focus on IS security development but on IS security analysis. This specialization allows a more detailed analysis so that the different foci of IS security analysis approaches can be identified and a more precise delineation of the approaches can be presented. The newly developed classification could prove useful to both researchers and practitioners in this field.

In the first section of the paper, "Research Approach", we describe the literature search, article selection, and article categorization processes we used. Existing IS security analysis approaches are analyzed in the "Related Work and Existing Literature Reviews" section. The results of the classification are presented in the section "Systematization of the Security Analysis Approaches". We outline a theoretical framework for systemizing and analyzing existing IS Security Analysis approaches in the section "Theory of the Framework". In our conclusion we summarize our key findings and provide recommendations for future work in this area.

RESEARCH APPROACH

The research approach used for the literature review was proposed by (Webster and Watson, 2002). A search was performed spanning IS security, information management, information systems, as well as risk and security management literature.

To identify relevant articles selected journals in these fields were examined by means of a full-text electronic search[1] using selected keywords such as "information systems security", "IS security (risk) analysis", "IS security (risk) assessment", and "security and risk management"[2]. This search identified a total of 465 articles. The titles and abstracts of each article were examined to determine their relevance for this research (i.e. the article related to the topic security analysis). This process generated 99 articles for in-depth review. In an effort to broaden the search beyond the original set of journals we used a snowball sampling technique (Goodman, 1961) and cited works of potential interest in those 99 articles were analyzed which yielded an additional 71 sources for our research. These sources included dissertations, master and bachelor theses, working papers from universities, conference proceedings, and publications from organizations and governmental agencies. In all a total of 161 articles were reviewed in-depth.

The categorization of the literature was concept-driven (Webster et al., 2002). Each article was examined to assess if it contained a suggestion for the systematization of security analysis approaches or already identified subclasses. Out of the 161 reviewed articles, 15 included such a suggestion. Table 1 identifies these articles and their area of focus. The table also shows which parts of the systematization are addressed by each article. An X in the column 'assessment approaches' indicates that the article addresses the systematization of assessment approaches. Astonishingly, two types of approaches – namely checklists or legislation accommodations - were not covered or mentioned by any of these articles.

Articles	Overall Systematization	Checklists	Assessment Approaches	Risk Analysis Approaches	IT Security Management Approaches	Legislation Accommodations
(Aagedal, den Braber, Dimitrakos, Gran, Raptis and Stølen, 2002)				X		
(Baskerville, 1993)	X	X				
(BITKOM, 2006)	X				X	X
(Dhillon and Backhouse, 2001)	X	X				
(Dhillon and Torkzadeh, 2006)	X					
(Eloff and von Solms, 2000)	X				X	X
(Faisst, Huther and Schneider, 2002)			X			
(Faisst, Prokein and Wegmann, 2007)			X			
(Gordon and Loeb, 2006)			X			

[1] The following databases were used: Business Source Premier, Science direct, JSTOR archive, INSPEC

[2] All issues of the following journals were searched in an effort to include leading journals in the selected disciplines and broaden the search in German-speaking areas: ACM Computing Surveys, ACM Transactions on Information and System Security, Bank Accounting & Finance, Communications of the ACM, Computers & Security, European Journal of Information Systems, HMD Praxis der Wirtschaftsinformatik, IEEE Security & Privacy, IEEE Software; IEEE Transactions Journals, IM Information Management & Consulting, Information and Organization, Information Management & Computer Security, Information Security Management, Information Systems Journal, Information Systems Management, Information Systems Research, Information Systems Security, Internal Auditor, International Journal of Network Management, Journal of Computer Security, Journal of Management Information Systems, Journal of Research and Practice in Information Technology, Journal of the Association for Information Systems, Management & Information Technologies, Management Information Systems Quarterly, Strategic Finance.

(Initiative D21)					X	
(Karabacaka and Sogukpinar, 2005)				X		
(Kokolakis, Demopoulos and Kiountouzis, 2000)				X		
(Siponen, 2005a)	X	X				
(Hoo, 2000)			X		X	
(Su, 2006)			X			

Table 1. Articles of Interest

RELATED WORK AND EXISTING LITERATURE REVIEWS

The literature review yielded five research publications that classify methods used in information systems security. These are the works of (Baskerville, 1993), (BITKOM, 2006), (Dhillon et al., 2001), (Eloff et al., 2000), and (Siponen, 2005b). Below we review each of these works and discuss what elements they bring to the classification scheme being developed and identify their shortcomings as relates to IS security analysis approaches.

(Siponen, 2005b) - An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice

(Siponen, 2005b) addresses information systems security (ISS) methods. His systematization consists of five classes (checklists, IS security standards, IS security maturity criteria, risk management, and formal methods), three of which are connected to IS security analysis. Two of Siponen's suggested classes, ISS maturity criteria and formal methods, are not security analysis approaches. Instead, their focus is on ensuring the secure development of information systems. The other three suggested classes are checklists, ISS standards, and risk management which correspond with the classes *checklist*, *IT security management approaches*, and *risk analysis approaches* which are suggested in the following paper. In contrast to Siponen's work the systematization developed in this paper distinguishes between standards and best practice models, which are subclasses of the IT security management approaches. Furthermore, in this paper the term risk analysis is used, instead of risk management. This is due to the fact that the focus of this paper is narrower than that of Siponen's work. Therefore, only risk analysis, which is part of the risk management, is of interest for this work.

Summary:

- Siponen's work addresses ISS Methods and therefore has a larger scope than our paper.
- Siponen suggests five classes which are somewhat disjointed. The five classes are not further subdivided which limits the decision support for the reader.
- Siponen does not consider legislation accommodation which impact IS security nor IS security assessment approaches.

(Dhillon et al., 2001) - Current Directions in IS Security Research: Towards Socio-Organizational Perspectives

(Dhillon et al., 2001) classify IS security by deriving four models from the fields of sociology and philosophy. Subsequently, various IS security approaches are assigned into these models. The IS security approaches they mention are, among others, checklists, risk analysis methods, and security evaluation methods where risk analysis is part of risk management. Because security analysis is only a part of security management, the class risk analysis is preferred to the class risk management as used by (Siponen, 2005b). The class evaluation is defined roughly: "Another category of research in computer security is in evaluation methods, whose rationale stems from the need to measure security" (Dhillon et al., 2001, 136). Approaches that they assign to this class include security models such as Bell-LaPadula as well as standards such as BS 7799. This particular systematization uses the term "standard" because security models are not appropriate for conducting a security analysis.

Summary:

- Dhillon and Backhouse examine socio-organizational aspects of information systems and IS security. Technical and economical aspects are not studied.
- Dhillon's and Backhouse's systematization classifies IS security methods according to the sociological and philosophical theories that they are based on. This approach is more scientific but is impractical for use in decision support.
- For sociological and philosophical purposes the classification can be considered complete but it is not suitable for IS security purposes. As mentioned, the technical and economical aspects of IS security are ignored in Dhillon's and Backhouse's systematization.
- Some of the content in this work is outdated. For example, the standard BS 7799 is no longer in use.

(Eloff et al., 2000) - Information Security Management: A Hierarchical Framework for Various Approaches

(Eloff et al., 2000) strive to distinguish and define terms in the field of IS security management. They identify and define the following terms: *standard*, *guideline*, *control*, *code of practice*, *certification*, *accreditation*, *benchmarking*, *self-assessment*, *legislation*, and *evaluation*. Examples for standards, guidelines, code of practices, and evaluations are provided and classified based on a framework the authors developed. The framework consists of two main classes: technology and processes.

Summary:

- Eloff and von Solms address IS security management approaches; whereas the focus of our paper is on IS security analysis.
- Eloff and von Solms only examine a few methods. Their work does not claim completeness.
- Their framework distinguishes two broad classes which are integrated. In contrast to Eloff's and von Solm's framework, the classification proposed in our paper consists of five classes and provides better decision support for the reader.
- The Eloff and von Solms article was written in 2000. Because of rapid developments in IS security, some parts of their work are now outdated.

(Baskerville, 1993) - Information Systems Security Design Methods: Implications for Information Systems Development

(Baskerville, 1993) compares the development of IS security analysis approaches with the development of IS development approaches by creating a framework which classifies approaches from both fields. The framework consists of three classes, which he labels *generations*. He classifies IS security analysis approaches chronologically and within the three generations he distinguishes between further approaches. Baskerville's work includes the classes *checklists* and *risk analysis approaches.* Cost-benefit analysis is suggested as a method to measure the economic aspects of security controls. However, the work does not cover IS security management approaches or the legislation accommodations which affect IS security.

Summary:

- Baskerville focuses on a systematization of IS security analysis and IS system development approaches. The topic is very similar to the work we present with the exception of covering system development approaches.
- Baskerville suggests a framework with three classes. The security analysis approaches are mapped to a corresponding generation class, based on their time of dominance. This chronological framework may not be a practical source of good decision support.
- Baskerville does not consider IT security management approaches nor legislation accommodations that affect IS security.
- Baskerville mentions cost-benefit analysis as a possibility for IS security assessment. We propose that there are considerably more approaches that could be useful for this purpose.
- Baskerville's article was published in 1993 and as such it is the oldest of the articles we analyzed.

(BITKOM, 2006) - Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk (IT Security Compass & Encyclopedia)

BITKOM is a federation of German IT (information technology), IS & IT-services industry organizations. As such it has worked on guidelines to provide companies with an overview of IS security standards and support them in the selection of relevant standards. The purpose of this article is similar to the other articles we reviewed and to our own paper, but the topics are different. For example, (BITKOM, 2006) considers *standards*, *best practice* models, and *legislation accommodations*, among others. Other standards which do not incorporate IS security analysis and assessment are also examined in the article. These include, for example, standards on physical security or cryptography. The article does not distinguish between standards and best practice models and only a selection of standards in each class are introduced. An important security management standard, NIST SP-800-30 (Stoneburner, Goguen and Feringa, 2002), is not addressed. A discussion on the impact of important legislation such as HIPAA (Department of Health and Human Services, 2005) is not provided.

SYSTEMATIZATION OF THE SECURITY ANALYSIS APPROACHES

This work aims to provide a comprehensive overview of IS security analysis approaches. In order to achieve this goal the works described in the section "Related Work and Existing Literature Reviews" were consolidated. By consolidating examples from the mentioned works and identifying IS security analysis approaches being discussed in recent publications we derived five categories (unambiguous classes) of IS security analysis approaches: *checklists*, *assessment approaches*, *risk analysis approaches*, *IT security management approaches*, and *legislation accommodations*.

The structure of the classification developed for this paper is based on the principles of grounded theory (Bennet, 1991). As proposed by (Glaser and Strauss, 1967) we sought possible classification classes from the ground up. First categories of occurrences and examples with common characteristics were identified and coded into as many classes as possible; second the attributes of each category were identified through constant comparison between occurrences and categories, so as to consolidate the classes; third the number of categories were reduced to a minimal set, i.e. no more occurrences were used than were needed to account for the distinguished classes; and finally the classification was used in a plausible representation of studied IS security analysis approaches.

All approaches in one class have same ideas or goals in respect to IS security analysis. Table 2 reiterates the connections between the systematization suggested in this paper and the scientific works described above[3].

Author	**Checklists**	**Assessment Approaches**	**Risk Analysis Approaches**	**IT-Security Management Approaches**	**Legislation Accommodations**
(Siponen, 2005a)	X	No particular consideration of IS Security Assessment Approaches	O	O	
(Dhillon et al., 2001)	X		X	O	
(Eloff et al., 2000)				O	X
(BITKOM, 2006)				X	X
(Baskerville, 1993)	X		X		
Legend: X means that the author uses the same name as in this paper. O means that the class can be found under a different name in the work of the respective author.					

Table 2. Systematization of other Scientific Articles

Figure 1 shows the identified classes of the systematization. The classes *assessment approaches*, *risk analysis approaches*, and *IT security management approaches* are further subdivided in subclasses. For each class we chose a representative method. These methods are the most important representatives of their respective classes because they are the most commonly used or best known.

Checklists are based on the idea that IT security solutions and procedures can be examined and written down in a list: a checklist. Examples of checklists include the American Federation of Information Processing Societies (AFIPS) checklist (Patrick, 1979), security audit and field evaluation for computer facilities and information systems (SAFE) (Krauss, 1972), Computer Security Handbook (Hoyt, 1973) and IBM's 88-point security assessment questionnaire (IBM, 1972).

In contrast to checklists, assessment approaches qualitatively or quantitatively assess risks and security controls respectively. Various methods from different research areas can be placed into this class. In order to enhance clarity, the assessment approaches are subdivided in two classes. One class contains approaches aimed at assessing risk; the other class contains approaches that assess security controls. (Faisst et al., 2002) classify the approaches to assess risk in the four classes questioning techniques, stochastic methods, indicator approaches and causal methods. The class questioning techniques contains all methods that use subjective estimation of people to assess risks. Questioning techniques are for example expert interviews as well as self assessments. With stochastic methods the assessment is based on already established methods from statistics and especially actuarial mathematics. The aim of these methods it to model loss distribution on the basis of historical data about potential loss due to IT risks. This should help to draw conclusions for effective risk management in the future. The conclusions are used for calculating the Value-at-Risk (VaR). Indicator approaches try to determine the existing risk on the basis of a certain indicator (single indicator approaches) or an indicator system (key indicator approaches). Causal methods focus on the modeling of the cause-effect-correlations of IT risks. Instruments of this approach are modeling techniques from physics, mathematics and computer science, which are already used and established in these fields for the design of processes and systems. Popular methods are neural networks, the Delta Method, and Bayesian networks.

[3] Not all of the examined approaches can be called security analysis methods. But because this paper aims to be comprehensive, both approaches that provide more than a security analysis and approaches that provide only parts of a security analysis are covered.

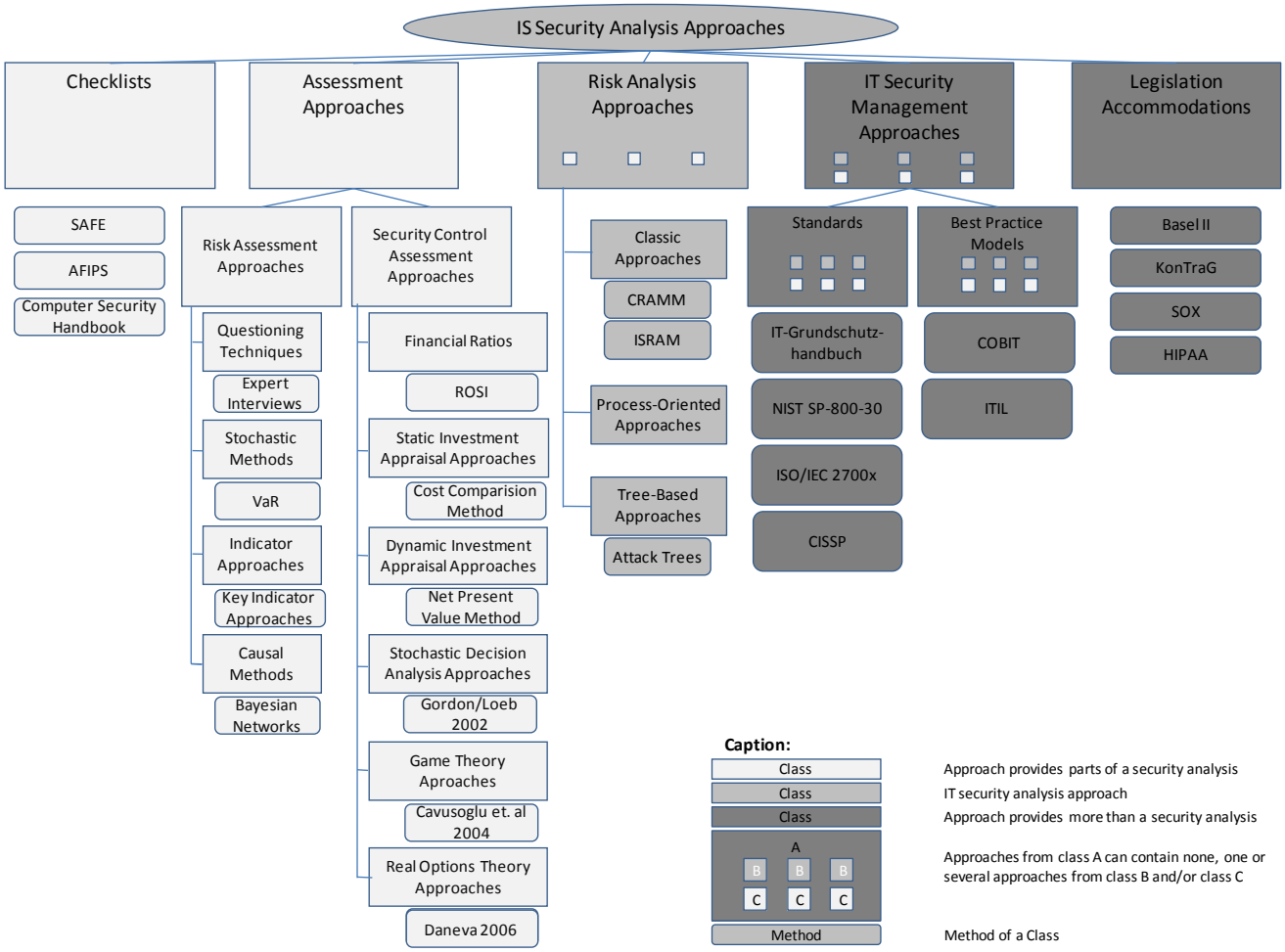

Figure 1. Systematization of IS Security Analysis Approaches

The approaches to assess security controls can be further classified in financial ratios, static investment appraisal approaches, dynamic investment appraisal approaches, stochastic decision analysis approaches, game theory approaches, and real options theory approaches[4]. A financial ratio is a ratio of selected values on an enterprise's financial statements. A common used financial ratio is the Return on Investment (ROI). The ROI puts the profit of an investment in relation to the invested capital. Investment Appraisal Approaches focus on optimizing investment decisions. Static approaches only examine one period. Dynamic approaches analyze and evaluate the financial impact of an investment over an entire investment period. A decision analysis model consists of a set of alternatives, one or more objective functions and a maximization goal. Because the incidence and the potential of the risks can not be determined ex ante, but are modelled with probabilities, the decision analysis models are considered stochastic. There are several published works, which follow this approach. Examples include the works of Bodin, Gordon and Loeb, 2005; Gordon and Loeb, 2002; Hoo, 2000; Longstaff, Chittister, Pethia and Haimes, 2000). Game theory is used to analyze problems in which the payoffs to players depend on the interaction motivated by players´ strategies. With security investment problem, the firm's payoff from security investment depends on the extent of hacking it is subjected to. The hacker's payoff from hacking depends on the likelihood of being caught. Based on the above idea, (Cavusoglu, Mishra and Raghunathan, 2004) use a game theory based approach to determine the optimal IT security investment level. The work of (Cremonini and Martini, 2005) also use this approach. Real options analysis was first developed as a decision support technique in the field of capital investment. There are, however, attempts to use real options to evaluate IT security controls. Gordon et al. (Gordon, Loeb and Lucyshyn, 2003) explain why a large portion of security

[4] The systematization is based on (Perridon, L., and Steiner, M. (2007) *Finanzwirtschaft der Unternehmung* Vahlen, München.) and (Su, X. (2006) An Overview of Economic Approaches to Information Security Management, University of Twente.).

expenditures seem to be made on a wait-and-see basis. (Daneva, 2006) proposes a real options-based decision framework for information security.

The purpose of a risk analysis is to analyze the security of the IT infrastructure, to compare it with the security goals and to draw consequences from the discrepancies. There are a vast number of risk analysis approaches. (LeVeque, 2006) distinguishes three classes: Classic (e.g. CRAMM[5]), process-oriented, and tree-based approaches (e.g. attack trees). IT security management approaches are often used to reduce the total expenditure for IS security. IT security management approaches support security officers in terms of methodology and content. However, these approaches contain more than the assessment of risk or security controls. They address the definition of security strategies and policies, the evaluation of security risk, the determination of security goals, the derivation of security requirements, the selection of appropriate security controls, and the implementation of these controls (BITKOM, 2006). IT Security Management Approaches can be subdivided in the two classes: Standards (e.g. ISO/IEC 27001, CISSP and IT-Grundschutzhandbuch) and Best Practice Models (e.g. ITIL and COBIT). Legislation accommodations affect a broad range of industries, ranging from finance to health care. Important examples of legislative policy that affect security management include Basel II, the Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), the Sarbanes-Oxley Act (SOX), and the Health Insurance Portability and Accountability Act (HIPAA) for healthcare system (Sunyaev, Leimeister, Schweiger and Krcmar, 2008).

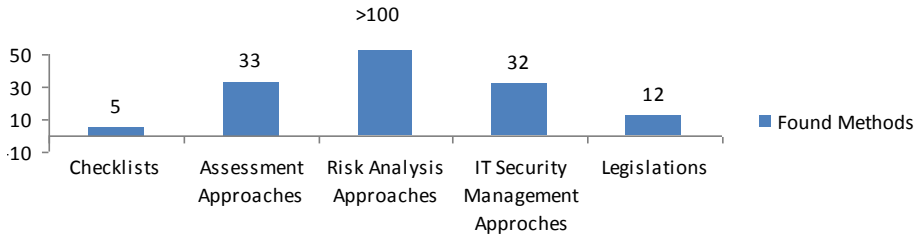

Figure 2. Found Methods in each Class

Checklists and assessment approaches only cover parts of a security analysis. Methods from these two classes can also be part of methods from other classes. For example a risk analysis method may consist of an assessment method and a checklist. In the same manner, IT security management approaches can include several methods from the other three classes. Legislation accommodations have an exceptional position. Compliance with regulations can be achieved by applying one or more approaches of the other classes. But legislation accommodations don't contain approaches of the other classes. Figure 2 illustrates the number of the methods found in each class.

THEORY OF THE FRAMEWORK

A central question of any review of the IS security literature is how to construct a classification scheme for existing IS security approaches (Siponen, 2005a). Through the literature review we found research publications that classify methods used in information systems security (Baskerville, 1993; BITKOM, 2006; Dhillon et al., 2001; Eloff et al., 2000; Siponen, 2005a). A difference between these classification schemes and the framework we propose is that the former concern the methods for the development of secure systems, while our paper focuses on the methods for the security analysis and assessment of information systems. The classification system proposed in this paper resulted from an iterative process involving the study of security topics in the IS field, analysis of prior work, and both refinement and incorporation of the elimination of the redundancy that arose due to the oftentimes confusing terminology (Eloff et al., 2000). (Siponen and Willison, 2007) perceived that "while there is no doubt that (existing IS security literature reviews) have provided a number of important insights for IS security research and practice, they have certain limitations". The advantages of the classification scheme presented here are that current IS security analysis approaches can be identified, compared, and assigned to one of the derived classes. The literature review is organized around an integrative framework that explicitly identifies the unique and unambiguous classes (as proposed in (Nosofsky, Clark and Shin, 1989)) of IS security analysis and assessment approaches. Consequently every approach that concerns IS security analysis can clearly be classified and identified within the introduced framework. When writing about a proposed framework or classification as a form of theory in IS, three primary criteria must

[5] CRAMM stands for CCTA's Risk Analysis and Management Methodology. The U.K. Government Central Computer and Telecommunications Agency (CCTA) set this method as standard risk analysis approach for all authorities in Great Britain (Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computmg Surveys*, 25, 4, 375-414.).

be met: (1) the framework must be identified; (2) relationships among the constructs in the framework must be specified; and (3) these relationships must be falsifiable (Gregor, 2006).

Class	**Distinguishing Attributes**
Checklists	Checklists cover part of a security analysis. No causal relationships to other classes.
Assessment Approaches	Assessment approaches cover parts of a security analysis. No causal relationships to other classes.
Risk Analysis Approaches	Risk analysis methods may consist of an assessment method and / or a checklist.
IT Security Management Approaches	IT security management approaches can include several methods from the first three classes.
Legislation Accommodations	Legislation accommodations have an exceptional position. Compliance with regulations can be achieved by applying one or more approaches of the other classes. But legislation accommodations don't contain approaches of the other classes.

Table 3. The Framework of IS Security Analysis Approaches

First, the results of our literature review suggested five main classes: *checklists*, *assessment approaches*, *risk analysis approaches*, *IT security management approaches*, and *legislation accommodations*. The distinguishing features of each class are shown in Table 3. All IS security analysis and assessment approaches can consequently be classified to one of these five classes. Secondly, most of the identified IS security analysis and assessment approaches provide only parts of an IS security analysis or provide only a method for an IS security analysis. This information influenced the considerations we made for introducing a classification which distinguishes between the classes which contain IS security approaches that are based on or contain either none, one or several approaches from preceded classes in our framework. There are three different kinds of classes. Classes that contain approaches providing parts of a security analysis, classes that contain IS security analysis approaches and classes that contain approaches which provide more than a security analysis. Hence, methods from some classes can be part of methods from other classes. Third, as already described above, our framework focuses on the structural nature of IS security analysis approaches which are defined parts of IS security management.

SUMMARY AND CONCLUSION

Our literature review indicated that none of the existing classification systems of security analysis methods covers all currently used approaches. This paper demonstrates a classification scheme that includes current state-of-the-art security analysis methods. The scheme provides a structured overview of current approaches and clearly indentifies the differences between them. This classification can therefore serve as a practical tool for security officers or IT security staff during the selection of suitable security analysis methods.

The classification scheme is tree-structured and consists of five primary classes. Each class contains approaches with similar characteristics. The five main classes are: checklists, assessment approaches, risk analysis approaches, IT security management approaches, and legislation accommodations. In addition, the five classes are also divided into subclasses.

In all, this paper aims to overcome the redundant terminology in the literature and provide a classification of IS security analysis and assessment methods. This new classification is related to previous publications but is more general in its focus and better able to identify and describe methods that are currently popular.

The results provide a basis for future IS security research. In the next step of our work we will concentrate on comparisons of the different approaches with the goal of identifying gaps in current IS security analysis approaches and further development of them.

REFERENCES

1. Aagedal, J.Ø., den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D., and Stølen, K. (2002) Model-based Risk Assessment to Improve Enterprise Security, Sixth International Enterprise Distributed Object Computing Conference, 2002, IEEE, 51- 62.
2. Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computmg Surveys*, 25, 4, 375-414.
3. Bennet, R. (1991) How is Management Research Carried Out?, in: *The Management Research Handbook,* N.C. Smith and P. Dainty (eds.), Taylor & Francis, Routledge, 1991, 318.

4. BITKOM (2006) Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin-Mitte.
5. Bodin, L.D., Gordon, L.A., and Loeb, M.P. (2005) Evaluating Information Security Investments Using the Analytic Hierarchy Process, *Communications of the ACM*, 48, 2, 79-83.
6. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) A Model for Evaluating IT Security Investments, *Communications of the ACM*, 47, 7.
7. Cody, E., Sharman, R., Rao, R.H., and Upadhyaya, S. (2008) Security in grid computing: A review and synthesis, *Decision Support Systems*, Vol. 44, Iss. 4; p. 749, Mar 2008.
8. Cremonini, M., and Martini, P. (2005) Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA), in: *4. Workshop on the Economics of Information Security (WEIS'05)*, Boston, USA, 2005.
9. Daneva, M. (2006) Applying Real Options Thinking to Information Security in Networked Organizations, Centre for Telematics and Information Technology, University of Twente., Enschede.
10. Department of Health and Human Services (2005) HIPAA Security Series - Basics of Risk Analysis and Risk Management, 2005.
11. Dhillon, G., and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *Info Systems J*, 11, 127–153.
12. Dhillon, G., and Torkzadeh, G. (2006) Value-focused assessment of information system security in organizations, *Info Systems J*, 16, 293-314.
13. Eloff, M.M., and von Solms, S.H. (2000) Information Security Management: A Hierarchical Framework for Various Approaches, *Computers & Security*, 19, 243-256.
14. Faisst, U., Huther, A., and Schneider, K. (2002) Management operationeller Risiken - Status, Systemanforderungen und Perspektiven (Teil 2), *Kredit & Rating Praxis*, 28, 4, 22-24.
15. Faisst, U., Prokein, O., and Wegmann, N. (2007) Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen, *ZfB*, 77, 511–538.
16. Glaser, B., and Strauss, A. (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research* Aldine Transaction, Chicago.
17. Goodman, L.A. (1961) Snowball Sampling, *Annals of Mathematical Statistics*, 32, 1, 148-170.
18. Gordon, L.A., and Loeb, M.P. (2002) The Economics of Information Security Investment, *ACM Transactions on Information and System Security*,, 5, 4, 438–457.
19. Gordon, L.A., and Loeb, M.P. (2006) Budgeting Process for Information Security Expenditures, *Communications of the ACM*, 49, 1, 121-!"%.
20. Gordon, L.A., Loeb, M.P., and Lucyshyn, W. (2003) Information security expenditures and real options: A wait-and-see approach, *Computer Security Journal*, 19, 1-7.
21. Gregor, S. (2006) The Nature of Theory in Information Systems, *MIS Quarterly*, 30, 3, 611-642.
22. Hoo, K.J.S. (2000) How Much Is Enough? A Risk-Management Approach to Computer Security.
23. Hoyt, D. (1973) *Computer Security Handbook* Macmillan, New York.
24. IBM (1972) *Secure automated facilities environment study 3, Part 2* IBM, Armnok.
25. Initiative D21 (2001) IT-Sicherheitskriterien im Vergleich.
26. Karabacaka, B., and Sogukpinar, I. (2005) ISRAM: information security risk analysis method, *Computers & Security*, 24, 2, 147-159.
27. Kokolakis, S.A., Demopoulos, A.J., and Kiountouzis, E.A. (2000) The use of business process modelling in information systems security analysis and design, *Information Management & Computer Security*, 8, 3, 107-116.
28. Krauss, L. (1972) *SAFE: Security audit and field evaluation for computer facilities and in-formation systems* Amacom, New York.
29. LeVeque, V. (2006) *Information Security - A Strategic Approach* Wiley-Interscience, Hoboken u.a.
30. Longstaff, T.A., Chittister, C., Pethia, R., and Haimes, Y.Y. (2000) Are We Forgetting the Risks of Information Technology?, *Computer*, 33, 12, 43- 51.
31. Nosofsky, R.M., Clark, S.E., and Shin, H.J. (1989) Rules an Exemplars in Categorization, Identification, and Recognition, *Journal of Experimental Psychology*, 15, 2, 282-304.
32. Patrick, R.L. (1979) *Security: Checklist for Computer Center Self-Audits* AFIPS.
33. Perridon, L., and Steiner, M. (2007) *Finanzwirtschaft der Unternehmung* Vahlen, München.
34. Siponen, M., and Willison, R. (2007) A Critical Assessment of IS Security Research Between 1990-2004, *15th European Conference of Information Systems, 2007*, St. Gallen, Switzerland, 1551-1559.
35. Siponen, M.T. (2005a) Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods, *Information and Organization*, 15, 4, 339-375.

36. Siponen, M.T. (2005b) An analysis of the traditional IS security approaches: implications for research and practice, *European Journal of Information Systems*, 14, 303–315.
37. Stoneburner, G., Goguen, A., and Feringa, A. (2002) Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology.
38. Su, X. (2006) An Overview of Economic Approaches to Information Security Management, University of Twente.
39. Sunyaev, A., Leimeister, J.M., Schweiger, A., and Krcmar, H. (2008) IT-Standards and Standardization Approaches in Healthcare, *Encyclopedia of Healthcare Information Systems*, Idea Group, 813-820.
40. Webster, J., and Watson, R.T. (2002) Analyzing the past to prepare for the future: writing a Literature Review., *MIS Quarterly*, 26, 2, xiii-xxiii.