Problem Analysis of Traditional IT-Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing Domain

Stefan Taubenberger, Jan Jürjens, Yijun Yu, Bashar Nuseibeh

Problem Analysis of Traditional IT-Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing domain

Stefan Taubenberger[1], Jan Jürjens[2], Yijun Yu[3], Bashar Nuseibeh[3, 4]

[1] MunichRe, Munich, Germany, Staubenberger@munichre.com
[2] TU Dortmund and Fraunhofer ISST, Germany, http://www.jurjens.de/jan
[3] Lero, University of Limerick, Ireland, y.yu@open.ac.uk
[4] The Open University, Milton Keynes, United Kingdom b.nuseibeh@open.ac.uk

Abstract. Traditional information technology (IT) security risk assessment approaches are based on an analysis of events, probabilities and impacts. In practice, security experts often find it difficult to determine IT risks reliably with precision. In this paper, we review the risk determination steps of traditional risk assessment approaches and report on our experience of using such approaches. Our experience is based on performing IT audits and IT business insurance cover assessments within a reinsurance company. The paper concludes with a summary of issues concerning traditional approaches that are related to the identification and evaluation of events, probabilities and impacts. We also conclude that there is a need to develop alternative approaches, and suggest a security requirements-based risk assessment approach without events and probabilities.

Keywords: IT risk analysis, IT risk assessment, Security requirements

1 Introduction

Companies and governmental organizations are interested in detecting and mitigating the risks of possible profit and image losses. Many quantitative and qualitative methods and toolkits for Information Technology (IT) security risk analysis have been developed using, such as normal probability, Bayesian probability, Fuzzy theories, Annual Loss Expectancy (ALE), all of which are based on probabilities and events as the risk is "measured in terms of a combination of the likelihood of an event and its consequence" in the ISO 27005 standard [19]. Estimating risks reliably with precision is difficult because of their unpredictability according to this definition: in each traditional risk assessment method or toolkit, probabilities about the events and the possible consequences have to be determined, and each of the steps to determine risk – identifying events, determining probabilities and impacts – has weaknesses, making risk assessments prone to errors, unreliable, and results questionable.
The objective of this paper is to discuss the general issues of determining risk with events and probabilities within traditional approaches. We report on our experiences

in IT risk assessments in the insurance and auditing domain. The main contribution of the paper is the thorough analysis of the problems of traditional risk assessment approaches based on the literature and our experiences. The paper is structured as follows: in section 2 we present problems of traditional approaches related to underlying methods and risk assessment steps. In section 3 we report on our problem experiences applying a traditional approach by hand on a real world example. We summarize the issues of traditional risk assessment approaches in section 4 and in section 5 we suggest developing alternative risk assessment approaches, such as based on security requirements and business process models.

2 Traditional approaches to IT-security risk assessment

In the literature many approaches for IT security risk assessment are available to researchers and practitioners. Discussions of available approaches can be found in Ralston et al. [23], Alter and Sherer [3], ENISA [7], and Putnam [21]. We discuss these methods from the perspective of the used underlying assessment methods (qualitative or quantitative), risk assessment activities, and the selection of assessment methods. In the following, we present our critiques based on a literature review.

2.1 Qualitative and quantitative methods

Quantitative risk assessment methods use numeric probability where the probability expresses the knowledge that the event occurs. With quantitative approaches risk is determined by the probability of an event and the likelihood of a loss. Examples of use of quantitative methods are: normal probability, Bayesian probability, Fuzzy theories and Dempster Shafer theory, Monte Carlo Simulation [15], Annual loss expectancy (ALE), and stochastic dominance [22]. The advantages of quantitative methods are that IT assets are identified most likely for damages [22], measures can be used for the impact magnitude and be directly compared [30], [8]. The disadvantages of quantitative methods are that there are no exact probability values of loss at the time when they are estimated and half of the estimates are statistically either too high or too low [22]. Furthermore, the probability function that usually follows a normal distribution may be deformed because it represents average values of a few extremes and many low ones [22]. Additionally, a scale has to be provided for what the value of “x” percent means [30]. These values have to be translated to a literal meaning.

Qualitative risk assessment methods use non-numeric values or number ranges to express the risk as descriptive values [22]. Examples for qualitative methods are: scenario analysis, fuzzy metrics, questionnaires [22], preliminary risk analysis (PHA), hazard and operability study (HAZOPS), and failure mode and effects analysis (FMEA/FMECA) [24]. The advantages of qualitative methods are that these approaches are time and cost efficient because no exact value has to be determined and they are valuable in estimating risk approximately [22] as well as areas of improvement can be easily identified [30]. However, the disadvantage of qualitative methods is that they are not precise as the value is expressed within a spectrum that

has to be understood by all involved parties [22]. Additionally, methods provide no measurement for the impact and therefore it is difficult to conduct a cost benefit analysis [30]. Although quantitative and qualitative methods can be combined and used together [17], results combination and interpretation become more difficult because different rating scales, underlying assessment principles or the variances in risk weighting are difficult to mix up.

2.2 Risk determination

In internationally accepted standards or methods like Octave [2], CORAS [29], AS/NZS 4360 [6] or ISO 27000 standards, the principal steps to determine risks are asset identification, event/threat identification, vulnerability/control identification, likelihood determination and impact analysis. Within the literature many issues of or critique on traditional approaches are provided. We can categorise all of these into three areas: identification, data and assessment.

(1) The *identification* category is about activities to determine, e.g. an event. A threat that uses vulnerabilities is defined as an event [19]. The identification of threats and vulnerabilities is challenging as underlying conditions change constantly e.g. development of new technologies, new competitors, new laws, etc. [16], [14] Therefore, threats and vulnerabilities are not static, with their behaviour and seriousness change within days. Threats and vulnerabilities are identified based on security expert knowledge, usage of security scanning tools and public available data. Security experts use implicit knowledge and experiences as well as explicit data such as vulnerability lists for the risk identification. But how do we know and how can we verify whether or not all threats and vulnerabilities have been identified correctly and completely? Furthermore, events in associated companies (e.g. outsourcing partners or inter-company process chain partners) could not be discovered as there are beyond company boundaries. However, these events could negatively affect a company as business processes and systems are heavily interconnected nowadays [16].

(2) The *data* category is about data needed for the evaluation of risks. For the impact and probability assessment of a risk, data regarding the impact and probability of event in a given situation for systems is needed. The major issues here are that exhaustive public available data of occurred events, impacts and their probabilities are not available [27], and the internal historic data are not available for the estimation of possible change impacts on the company. For example, the event has not occurred in this type of industry yet, within the company or the scope in this situation. If no comparable data is available, best guesses must be used for determining the change impact and probability. But how to make such a best guess in an environment where we do know little about the basic population to determine the occurrence rates, effects or the change impacts of the events? In case that event data is available, internal data about events in companies can still be incomplete or may represent a “lucky” history [9] and get quickly obsolete. In addition, internal historic event data may not represent a true view and events recorded could be lower-than-average [9]. For example, the claims data recorded regarding the occurrence rate and extent of loss is often below the average of the reference industry or competitors. Another issue is that probability

distributions get incorrect as they are based on historic data not representing event behaviour changes [28]. For example, the 100-year events reoccur nowadays for every 10 years in fat-tailed distributions. How can we ensure or verify that the data used for the assessment based on such data is still correct?

(3) The *assessment* category is about activities or models to evaluate the change impacts. Risk assessment is based on the impact and the probability of the event. The models used to determine risks and dependencies are poor because co-occurrence of risks, uncertainty between event relations and different assessment scales are not considered. Co-occurrence of events within different or the same risk leads to indeterminable impacts and damages because the events might occur in associated companies that may have an impact on other risks that are not considered when they are evaluated on their own. In current methods, the assessments are performed on decomposed model elements but do not consider the organization as a whole. Furthermore, there is uncertainty between the relation of an event and the impact by its nature. For example, the impact of the event is not known or dependent on other conditions/parameters. However, side effects (multiple impacts or dependencies) or parameters are not considered and uncertainty is assessed by gut feelings or subjective security expert knowledge [27]. Although safeguards put in place are considered in the impact assessment, they are evaluated for a particular threat/vulnerability, and the side effects of other events are not considered. How do we determine that safeguards are operated as intended? A systematic assessment of the safeguards regarding secure operation, secure design and effectiveness is currently missing. Furthermore, probabilities are measured by different techniques; for example, by quantitative and qualitative methods. But the comparability of qualitative and quantitative assessments of risks or probabilities within an assessment method is not validated. Furthermore, assessments are influenced by perceptions. Behavioural biases outgoing of the educational background, organizational level or positive/negative attitude of the assessor may affect the assessment of events, probabilities of occurrence or the impact estimation [16],[27],[25]. In addition, current risk assessment proceedings lead to simplification and are focused to strong on technical issues rather than on information or business issues [11]. For procedural reasons the assessor will usually simplify otherwise he will be lost in detail and forget the objectives [12]. Additionally, methods follow the waterfall model and therefore are not capable of considering changes during the lifetime of the assessment [31].

2.3 Selection and classification of IT-security risk assessment methods

In the literature many approaches for IT security risk assessment are available by researchers and practitioners and in general "published work related to risk assessment is very difficult to categorize." ([23], p.6) and "There are more than 200 risk management methods making it a challenge to select the most adequate one" ([18], p.1). These difficulties to categorize and select an appropriate risk assessment approach arise because the risk assessment process consists of different phases namely: risk identification, risk analysis, risk assessment (evaluation and ranking) and risk management (treatment and mitigation), and developed approaches cover different phases as well as concentrate on different aspects, problems or business

areas. An issue in classifying approaches is to determine how much of the risk assessment process is covered by the proposed approach. Another issue is the great variety and profundity of the approaches and their description how they perform and to apply in a given situation. Researches tried to classify approaches like Campell and Stamp [5] who provided a classification scheme consisting of two dimensions "level" and "approach" divided further into subcategories, however lacks a classification regarding the elements of the risk assessment approach. The five basic classes used by Siponen [26] misses any further distinguishing characteristics and are therefore not expedient for a classification. In an ENISA working group paper [1] as well as in the thesis of Poettinger [20], risk exposure, risk impact and impact segment are used to determine the most appropriate risk assessment methodology. Although Spider diagrams are used to compare the methods with organizational requirements, currently there is no general accepted and proven classification scheme in existing approaches. Further on, developed or criticized approaches are typically not classified or categorized making it hard for researches to apply the approach in the correct setting or to select the most appropriate one.

3 Our experiences with traditional approaches

In Information System (IS) audits as well as for providing insurance cover for business interruptions auditors have to evaluate IT risks. They evaluate IT systems, processes and risk prevention capabilities. The purpose of these risk assessments is to determine significant risks that are associated with the design, implementation and operation of IT systems of a company. The audit committee or the insurer commissions these assessments. The audit team presents these significant risks to the management or underwriters and reports to the audit committee or insurer. The significance of risks is determined qualitative by the impact of the threat and the results are used to decide about risk acceptance/ mitigation or about insurance cover. However, auditors face the problem that data about events, probabilities are rarely available in public or in the company assessed. Furthermore, these audits have to be cost and time efficient and the results should be reliable regarding future events to acquire profitable business as well as for the annual financial statement.

3.1 IT-security risk assessment with a traditional approach

In this section we describe the context and the results of applying a traditional approach on a simplified real world example.

Context: We have applied a proven traditional approach such as [30] more than ten times to determine IT security risks in subsidiaries and branches of a reinsurance company within audits as well as at companies that applied for business interruption insurance. These assessments conducted by an IT auditor and an independent security expert, focus on IT management, systems, and normally last one week. The assessment team is independent of the IT operation or IT management of the assessed company or branch. IT departments of different sizes and organizational forms were

assessed. In a centralized environment the assessments stopped at the service interface; however service quality and service agreements were considered.
Approach selection: We selected the NIST 800-30 approach [30] because it is well known and documented, learnt in less than three days [4] and the tendency to rate threats as medium or low [4]. Especially, the tendency to have a few high risks is important to direct management/companies efforts to the most critical issues.
Limitations: With risk assessments not all risks may be identified neither can we guarantee that. However, we adjusted our assessments to identify significant risks regarding best practices within a confidence level of professional experience.

The following is a simplified real world example: The main sales channel of an internet retailer for clothes is their online web store. The customer has to provide all shipping and payment data before an order via the online store is processed. Customers can make payments by credit card or on delivery. After providing and verification of all necessary data, the order is stored and processed. The web store is a web application with a connected database containing all order data and has an interface to a third party service to verify credit card data. As we have thorough knowledge about vulnerabilities, we know that the web application has an SQL injection problem and an encryption problem in the communication with the costumer and third party service.

An IT security risk assessment with a traditional approach such as [30] would proceed with asset- , threat-, vulnerability- and impact-analysis to determine risks.
(1) Asset identification and analysis: Hardware, software, data, people have to be identified as well as their criticality or value to the organization. In our example we identified the online web store, the external service provider, customer, credit card and order data. People involved include customers and order handling personnel.
(2) Threat identification and analysis*:* All potential threat sources have to be identified. We identified natural disaster threats such as tornados, floods and earthquakes, and human behaviour threats from hackers, computer criminals, terrorists or espionage and insiders/disgruntled employees. Technical threats include blackouts, fire, and chemical pollution.
(3) Vulnerability identification and analysis: All weaknesses that can result in security breaches in the system security procedures, design or operation have to be determined. A system design analysis revealed that the web server application has an SQL injection problem and that the communication with the database is unencrypted. The external service provider was not analysed as an external report showed no vulnerabilities. Employees were not considered as vulnerable as there is no customer contact and no indications of disgruntled employees.
(4) Likelihood determination and impact analysis: The impact and the likelihood of a successful security breach have to be determined with regard to the criticality of the asset. The probability ratings were defined as low (0-30%); medium (30-70%) and high (70-100%). The impact scale was defined as low (<1 million Euro), medium (1 to 5 million Euro) and high (>5 million Euro).

Natural disaster threats were not considered because the data centre is not exposed and estimated probabilities are < 1 percent. The power blackout from the technical threats was rated as probable (low) but with low impact. Fire is no risk as it is treated by a sprinkler system. Chemical pollution was rated as unlikely. The web server

encryption issue was rated with low probability for criminals, medium for hackers and the impact was rated medium for both. The web server injection issue was rated with low probability and medium impact. Terrorists and espionage was not considered because the business is not critical. Table 1 shows some of the risk ratings.

Table 1. Risks and risk ratings in our scenario.

Traditional approach		
Risk	**Probability**	**Impact**
Power Blackout	Low	Low
Web server encryption criminal	Low	Medium
Web server encryption hacker	Medium	Medium
Web server SQL injection	Low	Medium

3.2 Methodological and Estimation problems

In the following we describe general and probability estimation issues we experienced by applying the steps of the NIST 800-30 [30] approach. In the ***asset identification phase***, the business process is decomposed into single elements. But any dependencies between elements are neither considered nor modelled. In the ***threat and vulnerability identification phases*** the main problem is uncertainty. We do not know whether the threats listed or the identified vulnerabilities are complete and comprehensive and how to verify them. We are dependent on publicly available data and the assessor knowledge and experience. For the ***likelihood determination and the impact analysis of threats*** there is no detailed guidance available. For example, NIST 800-30 does not describe how to link threat sources with vulnerabilities and how to derive or evaluate any probabilities. Our probability estimates may not represent a true view as the behaviour of attackers and defenders changes. The aggregation of probability values causes further problems as the probability of occurrence might be misrepresented. In addition, the consequences and the existence of misestimating are not considered. Misestimating or unknowingly influenced assessors [27] as well as the existence of ambiguity and the aggregation of risk creates an estimation risk that is not considered. As a result, events and impacts may be under-/over-represented.

In what follows we demonstrate the divergence of probability estimates. Therefore, we try to verify our probability ratings of section 3.1. We attempt to determine the probability that a malicious user exploits the encryption weakness of the web server and the probability not exploiting any weakness. For determining these probabilities the following parameters should be considered:

- Number of known exploits and not secured exploits for the web server version: Determinable by publicly reported bugs/vulnerabilities and a security analysis.
- Criticality of exploits: Determinable as exploits are rated.
- Detection rate of all vulnerabilities by malicious user: Not determinable as the ratio is dependent on the knowledge of vulnerabilities, the used/ available tools and number of exploits/ vulnerabilities available.
- Number of users: Determinable by page views and IP-address matching.

- Ratio of successful exploiting: Not determinable as the ratio is dependent on malicious user's knowledge, the complexity of vulnerabilities as well as the motive, resources and time of the malicious user.
- Relation of friendly and malicious users accessing the web server: Not determinable and dependent on e.g. popularity of the company, monetary gain.
- Impact of controls: Is implicitly considered in the successful exploiting ratio.

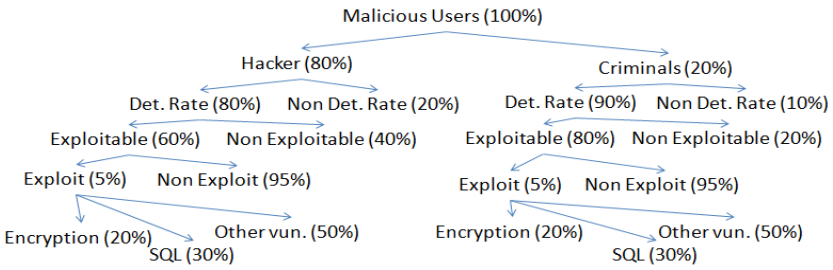

Fig. 1. Dependency tree with probability ratings

A parameter tree showing dependencies and assigned probabilities values for our example in section 3.1 looks like figure 1. The percentages in the probability tree were assigned by us based on available data and estimates. The probabilities for events as asked in the beginning are as follows, if one computes the probabilities down the probability tree for a hacker or a criminal.

- A criminal exploits the encryption weakness in the web server in 0.144%.
- A hacker exploits the encryption weakness in the web server in 0.384%.
- A malicious user exploits the encryption weakness in the web server in 0.528%.
- The likelihood that a malicious user does not exploit any weakness is 97.36%.

The values express the probability of occurrence of exploiting the vulnerability by a malicious user. Notice, that there is a major discrepancy between the results of section 3.1 and this calculation. These result variations maybe caused by us because of bad estimates or mistakes. Therefore, we also tried changing ratios besides the variations while we recognized the following:

Dependencies: There is a direct dependency of the result to single parameters e.g. a reduction/increase of one parameter from 5 to 10 (100 percent change) leads to a reduction/increase of the result in the same percentage. We recognized that the percentage of misestimating is relevant not the absolute amount.

Baseline: The total population has to be specified because a, for example, 12% or medium probability has no significance. This is especially important when populations are linked like the malicious users to normal user's ratio.

Probability: In a chain of parameters the total probability inclines against 0 or 100 percent as it is below or above the minimum or maximum values. These high or low values blur the total probability exceptionally.

Tree diagram: Generally, it is difficult to determine the dependencies of parameters, the correct tree diagram and to verify the diagram as there is no data available.

Perception: The perception of the results is dependent on the probability question and the result value. A higher percentage and positive statement (e.g. an event is 80 percent likely instead of 20 percent unlikely) is assumed to provide more confidence.

3.3 Result presentation and perception

Traditional approaches present risks as threats or threat diagrams. Categories such as high, medium and low indicate the severity and probability of the threat like shown in table 1. However, without further information, like basic population, countermeasures costs, required security, and effects on operations and the security of the application, data or transaction, a reasonable decision on risk mitigation or acceptance is hardly possible. Furthermore, the decision on risk mitigation or acceptance is a second assessment influenced by subjective factors and on individual's perception of risk [27] representing constraints to countermeasure implementation.
Risk attitude and perception: The perception of risk is influenced by e.g. personal experiences, media, social groups [27] as well as a person's risk attitude - risk taker vs. risk aware person.
Frequency: Countermeasure implementation is dependent on costs, impact, probability and frequency. But the frequency in a period of time is not specified in the risk analysis results.
Cost objectives: The implementation of measures depends on company internal cost objectives as personal or departmental objectives may not be accomplished. Furthermore, measures that are not planned in the current year budget may not be implemented immediately.
Prioritization: Business critical projects or security issues in daily operations have a higher priority than proposed countermeasures as an event has materialized.

All these factors are influencing the overall assessment results and arise due to the representation of risk and the possibility to interpret results. As a result the optimal security level is not achieved and the company's security standard was defined, changed (without notification) or violated by the acceptance of risk.

4 Problem analysis - summary

In the literature review as well as through our experiences we have identified a number of issues related to used methods and activities in traditional risk assessments.
Methods: Quantitative methods base on data that is not reliable available in practice with a certain precision and qualitative methods provide results within a range with deviations that have to be interpreted. Interpretation is subject to misjudgment and the selection of an approach in a given situation is not supported by any of the developed methods making it difficult to choose the appropriate approach.
Guidance and identification: Current standards are missing guidance on likelihood determination, event correlation and linking of threats, probabilities and impact. However, such guidance would be highly beneficial for risk analysts. The concept used for identification of, threats, vulnerabilities or correlations "you know one when you see one" applied in most methods does not work on new risks as this concept is based on implicit experience, thresholds and occurred damages.
Dependencies: In current approaches, the assessor conducts the risk assessment on decomposed single model elements. However, that proceeding neglects design or interrelated risks as well as organizational coherences.
Probabilities: The assessor mostly estimates probability values in assessments, as

there is no reliable and true data. But estimates are mostly biased, statistically incorrect or the data base of the distribution might be incorrect because of behavioural changes or a "lucky" history. In addition, we experienced that already small derivations or unconsidered parameters such as the timeframe or total population have a material impact on the result. There is no feasible way to verify the correctness and completeness of probability dependencies (tree) and positive and high probability statements are perceived as more trustworthy by people.
Assessment: Assessments are conducted on uncertainty regarding events, probabilities and impact. However, uncertainty, co-occurrence as well as dependencies are not modelled and properly considered. Furthermore, assessments are specific to a point of time not considering environment changes or prevention capabilities of the company.
Risks results: We experienced that low and a few medium risks were not mitigated because of personal and company specific constraints such as perception, cost objectives and prioritization of activities. Furthermore, the impact on the companies security level or polices is not appropriately considered when risk is accepted.
Environment: To identify and to determine events, probabilities and impacts correctly we must have comprehensive knowledge about the environment of the risk, the company and outside world. This would require that all parameters, corresponding probabilities, the basic population as well as correlations are known, are immediately updated, base on enough statistic data and could be modelled. But comprehensive knowledge about the environment is not available, may be compromised, cannot be verified and cannot be modelled as the real world is too complex and unpredictable. This applies to all risk assessments and is not specific to our problem domain. Furthermore, risk is about people. Their behaviour is not objective or rational, may follow personal interests or herd-instincts and be biased.

5 Conclusion

Due to the nature of risk - its unpredictability and complexity - risk assessment is difficult. Our problem analysis of traditional approaches based on the literature and our experiences in the insurance and auditing domain showed that such issues like uncertainty, wrong estimation and perception are mainly associated with determining events, probabilities and change impacts, affecting adversely the risk results. We therefore suggest that future approaches should attempt to determine risk by alternative concepts.
One possible and promising direction is to use security requirements (SR) [10], [13] not only for determining the impact of a threat or the seriousness of vulnerabilities but considering organizational needs in the risk assessment. An alternative risk assessment approach with SR could manage to determine risk without using events and probabilities and considering the organizations capability to handle and prevent events. This could be achieved, for example, by specifying the business process data security needs and by evaluating these requirements by hand of process model activities concerning the actors related to the system. Security requirements and corresponding security controls are evaluated at individual process activities for validating whether or not the system implementation, the actor's process activities

(operation) and the process design adheres to the requirements. In addition to business process evaluation, IT process maturity and performance are evaluated to detect weaknesses, to determine operating effectiveness and prevention capabilities. The IT process evaluation results can be used to evaluate the adherence of business process data security requirements from an infrastructure perspective as well as to indicate the time invariance of the risk results. However, to determine risks only using security requirements without having to determine events and probabilities would lead to a redefinition of risk as "the non-adherence of security requirements thereby causing harms to the organization regardless of a point in time". An advantage of such an approach would be that assessment results are more time independent and results probably more accurate and linked to organizational security needs. Before developing such an approach we believe we need a better understanding of the interaction of security requirements, risk treatments, risks, assets and assurance as a foundation. We are confident that a security requirement based approach has the potential to overcome the limitations of traditional approaches and we hypothesise that an entity would face no substantial risks from any events/threats if the evaluated security requirements have been adhered to.

Acknowledgement. Supported, in part, by the EU as part of the SecureChange project and SFI grant 03/CE2/I303_1.

6 References

[1] ENISA 2007-2008 ad hoc Working Group on Risk Assessment/Risk Management. Determining your organization's information risk assessment and management requirements and selecting appropriate methodologies, 2008.

[2] Alberts, C., Dorofee, A., Stevens, J. and Woody, C.: *Introduction to the OCTAVE Approach*. Carnegie Mellon Software Engineering Institute, Pittsburgh, USA, August 2003.

[3] Alter, S. and Sherer, S.: A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems*, 14:1–28, 2004.

[4] Buyens, K., DeWin, B. and Joosen, W.: Empirical and statistical analysis of risk analysis-driven techniques for threat management. IEEE Computer Society, 2007.

[5] Campbell, P. and Stamp, J.: A classification scheme for risk assessment methods. SANDIA REPORT, SAND2004-4233, 2004.

[6] Australian/New Zealand Standards Comittee. Risk management ASNZ 4360:1999, 1999.

[7] ENISA. Inventory of risk assessment and risk management methods, ENISA ad hoc working group on risk assessment and risk management, March 2006.

[8] Feather, M. and Cornford, S.:. Relating risk and reliability predictions to design and development choices. In *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS), Newport Beach, CA, 23-26 January, 2006.*

[9] Frachot, A. and Roncalli, T.: Mixing internal and external data for managing operational risk, 2002.

[10] Gerber. M. and von Solms, R.: From risk analysis to security requirements. *Computers & Security*, 20:577–584, 2002.

[11] Gerber, M., von Solms, R. and Overbeek, P.: Formalizing information security requirements. *Information Management & Computer Security*, 9(1):32 – 37, 2001.

[12] Halliday, S., Badenhorst, K. and von Solms, R.: A business approach to effective information technology risk analysis and management. *Information Management &Computer Security*, 4(1):19–31, 1996.
[13] Houmb, S. and Jürjens, J.: Developing secure networked web-based systems using model-based risk assessment and UMLsec. In *10th Asia-Pacific Software Engineering Conference(APSEC 2003)*, Chiangmai (Thailand), 10-12 December 2003.
[14] Jackson, M.: NII-OU Security Workshop @ The Open University, November 2007.
[15] Kaplan, S.: The words of risk analysis. *Risk Analysis*, 17(4), 1997.
[16] Kinney, W.: Research opportunities in internal auditing - chapter 5 auditing risk assessment and risk management process. *The Institute of Internal Auditors Research Foundation,* 2003.
[17] Zhang, Y., Jiang, S., Cui, Y., Zhang, B. and Xia, H.: A qualitative and quantitative risk assessment method in software security. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, volume 1, pages V1–534 –V1–539, 2010.
[18] Matulevius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P. and Genon. N.: *Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development*, pages 541–555. Springer Publishing, 2008.
[19] International Organization of Standardization (ISO). ISO 27005 Information technology - Security techniques - Information security risk management, International Organization of Standardization (ISO), 2008.
[20] Pöttinger, J.: Self assessed risk management. Master's thesis, Fachhochschul-Masterstudiengang Sichere Informationssysteme, 2009.
[21] Putnam, A., Kreitner, C. and Rasmussen, M.: Information security management references, available at www.theiia.org/download.cfm?file=1319, 2004.
[22] Rainer, R., Snyder, C. and Carr, H.: Risk analysis for information technology. *Journal of Management Information Systems*, 8(1):129–147, 1991.
[23] Ralston, P., Graham, J. and Patel, S.: Literature review of security and risk assessment of SCADA and DCS systems, Technical Report TR-ISRL-06-01. July 2006.
[24] Rausand, M.: *System Reliability Theory (2nd ed)*, chapter Risk Analysis An Introduction. Wiley, 2004.
[25] Redmill, F.: Risk analysis - a subjective process. *Engineering Management Journal*, 12(2):91–96, 2002.
[26] Siponen, M.: An analysis of the traditional is security approaches: implications for research and practice. *European Journal of Information Systems*, 14:303–315, 2005.
[27] Stewart, A.: On risk: perception and direction. *Computers & Security*, 23:362–370, 2004.
[28] Stiglitz, J.: Making globalization work: Global financial markets in an era of turbulence. Frankfurt, February 2008.
[29] Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B.A., Houmb, S., Lund, M., Stamatiou, Y. and Aagedal, J.: Model-based risk assessment – the CORAS approach. In *NIK (2002) informatics conference, Kongsberg*, 2002.
[30] Stoneburner, G., Goguen, A. and Feringa, A.: *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, July 2002.
[31] Vidalis, S.: A critical discussion of risk and threat analysis methods and methodologies. Technical Report CS-04-03, University of Glamorgan, Pontypridd, 2004.