A Taxonomy of Challenges in Information Security Risk Management

Gaute Wangen & Einar Snekkenes
NISlab Norwegian Information Security laboratory, Høgskolen i Gjøvik
Gaute.Wangen2@hig.no Einar.Snekkenes@hig.no

Abstract

Risk Management is viewed by many as the cornerstone of information security and is used to determine what to protect and how. How to approach risk management for information security is an ongoing debate as there are several difficulties in existing approaches. The problems and challenges within the discipline are not easily visible being dispersed throughout literature. There is therefore a need for an overview for both industry and researchers to obtain a holistic picture of the research area and to contribute in making progress. In this paper, we present a taxonomy of identified problems from literature within information security risk management, and highlight some of the important prevailing issues that are contributing to lack of progress within the research field.

1 Introduction

The main goal of information security (IS) is to secure the business against threats and ensure success in daily operations[3] by ensuring confidentiality, integrity, availability and non-repudiation. Best practice information security (IS) is highly dependent on well-functioning risk management (RM) processes[10, 40], and RM is often viewed as the cornerstone of IS[41]. Information security risk management (ISRM) is the practice of continuously identifying, reviewing and monitoring risks, to obtain and maintain risk acceptance[4].

ISRM is a complex field with many unsolved problems; some make the claim that the current state of risk management is that it is broken and does not work[24], while others take it a step further and claim that the current qualitative risk management practices are actually worse than having nothing[22]. We believe that an understanding of the underlying reasons that are causing problems is essential for the scientific community and industry to be able to make progress. Due to the complexity and interconnections in the research field, researchers should avoid addressing one isolated problem at a time while ignoring the remaining challenges. However, the known problems in the ISRM research field are not easily visible being dispersed throughout the scientific literature. There is therefore a need for an overview of the current problems and challenges in the

This paper was presented at the NISK-2013 conference; see http://www.frisc.no/.

discipline to support a more holistic approach to ISRM research.
In this article, we have collected a non-exhaustive compilation of ISRM and Risk Analysis (ISRA) problems highlighted in published literature. We present a taxonomy based on current best practices for ISRM to aid in identifying prevalent problems, and for sorting current challenges in the research field. This article will therefore be useful in a setting where the reader need an overview of the current issues in the research field and of the known theoretical causes of problems in the ISRM practice.
We organize this article as follows. In section 2 we introduce existing works on ISRM taxonomies. Section 3 describes our taxonomy of ISRM challenges and findings. Section 4 contains a discussion and analysis of the results, and section 5 states the conclusion.

2 Related Work

Syalim et.al. [36] provides a comparison of four established risk analysis methods. As a basis for comparison, the paper provides four basic steps of risk analysis, being Threat identification, Vulnerability Identification, Risk Determination, and Control Recommendation. The framework proposed by Bornman and Labuschagne[11] was created to aid organizations in choosing a ISRM method. The comparison uses detailed versions of three criteria; Risks, Management and Processes, which in short represents what, who and how. Ekelhart et.al.[15] highlights the need for a security ontology, a ”common language” for IS professionals to ease communication and help achieve a common understanding of IS across companies and borders. Another purpose of the ontology is to improve the existing quantitative risk analysis. ”The Risk Taxonomy” is a technical standard provided by the Open Group[2], and is a document that offers a standard definition and taxonomy for IS risk to help combat the growing language gap between professionals. It also provides a model that contains a set of requirements and factors that all new risk assessment approaches should include.
Behnia et.al.[8] has published a survey of ISRA methods, which also contains a comparison of several of the popular ISRM methods. The presented framework for comparison is based on criteria such as if the method has supporting tools, vendor name, country of origin, etc The purpose of this comparison framework is to assist practitioners in choosing an ISRM for his organization.
ENISA[1] rate several different ISRA approaches according to quality. The report also contains an overview of methods that contain ISRM steps. ENISA also addresses the skills needed for conducting each method.
Campbell and Stamp[13] present a classification scheme where ISRM methods are sorted in a 3-by-3 matrix. The scheme sorts methods by level of detail and type of approach. This scheme provides practitioners an inkling to what skill level is required, intrusiveness, and the kind of method (e.g. compliance testing or audit).
Snekkenes[35] presents a taxonomy of ISRM methods using the view of key building blocks in ISRM methods. The taxonomy sorts ISRM into five activity classes for distinguishing and comparing methods. Snekkenes also presents a research menu for ISRM issues and research challenges.

3 A Taxonomy of Challenges

The main purpose of our taxonomy is to categorize and present findings at different stages in the ISRM areas and activities. Several of the existing ISRM/ISRA taxonomies have been made to help professionals choose method[11, 8, 1, 13], while others exist to improve certain research problems[2, 15], and for comparison of methods[35, 36]. The taxonomy presented in this paper was created reusing some of the criteria from ENISA[1], together with information collected from the scientific literature survey of existing ISRM methods and frameworks (such as[4, 23, 14] and many more). The main classifications chosen for our model are steps that are present in some form in many ISRM models. The taxonomy includes all the ISRM steps from ISO/IEC 27005:2011[4], and we have chosen to use the vocabulary established by ISO/IEC[3]. The taxonomy is presented top-down model using levels and is illustrated in figure 1. We have grouped similar findings within each category.

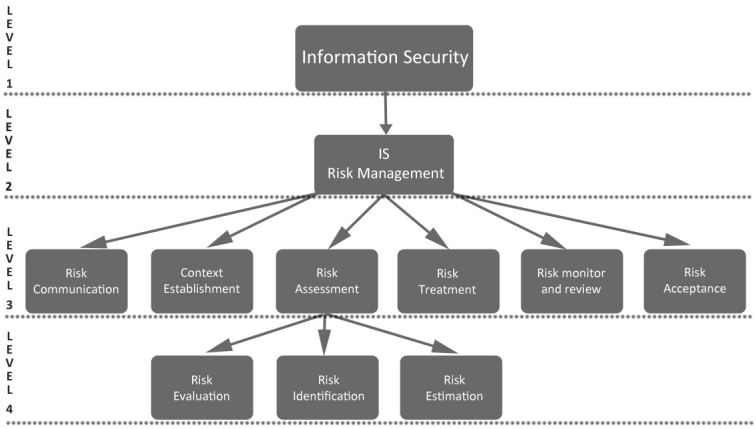

Figure 1: The Taxonomy of Challenges in ISRM

- **Level 1, The Information Security Category:** This category contains high-level findings in information security that affect ISRM, these findings did not fit sensibly into the taxonomy because of being a more wide spread issue.
- **Level 2, The IS Risk Management Category:** This category contains general findings in ISRM/RM that did not fit into any of the RM activities in level three of the model.
- **Level 3, The Different Risk Management Categories:** This level contains a classification for all of the identified ISRM activities (see figure 1). The findings from the survey are categorized within the activity that they are performed.
- **Level 4, The Risk Assessment Category:** This level contains the findings for the risk assessment category, sorted in the two risk analysis activities ”Risk Identification” and ”Risk Estimation”, and ”Risk Evaluation”.

Level 1, Information Security

Biased Scope and Misconceptions

Blakley et. al.[10]claims that the discipline of IS is generally more concerned with technical security, which can represent a problem as technical security only represents

a small part of the IS risks. Siponen[32] claim that traditional ISRM methods have been dedicated to evaluating technological aspects and to some degree disregard risks within human performance. Which makes it a challenge to detect and treat risks within human performance, human errors, and organization wide factors[9]. While Ozkan and Karabacak[28] point to a similar misconception: such as IS being a purely technical task that can be successfully performed by the IT department only, IS is company-wide and the IT department in general does not have sufficient power to run such a program and seldom have a holistic view of the organization. The same authors also highlight the misconception that consultancy firms can and should achieve IS management for an organization.

Common IS Language
Ekelhart et.al[14] highlights the need for a common IS language, as the language gap leads to confusion among experts, the people and organizations. The Open Group[2] also comments on the language gap that has evolved between businesses, and state that a common, logical and effective understanding of the fundamental IS problems are required in order for the IS profession to evolve significantly.

Conflicting Incentives and Human Factors
Hagen[17] points to the lack of incentives to report incidents which present a problem in IS. The people that incidents happen to (or cause them) may have many incentives not to report them, leading to underreporting and lack of knowledge regarding the effectiveness system controls[17, 10].
Hubbard[22] comments on the development gap between RM methods, and refers to the problem as a lack of communication between developers. Another problem identified by Hubbard is what he refers to as the over selling of methods that have no proven effect driven by a financial incentive and undermining more theoretical methods that work[22]. The ”perverse” economic incentives is also commented on by Anderson[6].

Lack of Empirical Research and Good Data
The majority of the relevant IS and ISRM literature is based on opinion, anecdotal evidence, or experience[25]. Blakley et. al.[10] explains that ISRM professionals do not have sufficient training to design experiments and publish results. The difficulties in obtaining empirical data and conducting IS research is also because of IS being one of the most intrusive types of research that can be conducted[25].

Lack of Validation and Testing
Blakley et.al. [10] states that there is little or no independent testing of IS measures and controls, which leads to lack of knowledge regarding the effectiveness of security measures. Not sharing test data leads to lack of available data for others, and *”...the results of effectiveness testing done by vendors and their contractors are almost never published”*[10]. Blakley et.al. further claim that security technology has a low effectiveness. Hubbard[22] points out that the methods that are developed lack rigorous scientific testing or mathematical proof.

Level 2, ISRM

Biased Scope and Misconceptions
Harris[18] points to the tendency of practitioners to have a technical scope and focus more on applications, devices, viruses and hacking. She also states that not enough practitioners

understand RM and are able to calculate risks and map them to business drivers.
Jaquith[24] points to some misconceptions in mainstream ISRM. He states that the current practice in ISRM misses the important parts and purpose of RM, which are quantification and valuating risk. For most people RM really means ”Risk Identification”, and that many view security as a product, while it should be viewed as a process.
The ”Something is better than nothing” is according to Hubbard[22] a misconception. He further explains that having something is not always better than having nothing. If the organization can not prove that the ISRM program works, it may be worse than having nothing. Money and resources are spent on something that can have zero impact on the organizations business, and failed ISRM may even leave the organization worse off than it was to begin with.

Existing RM methods
Subjective Scoring Methods and Risk Matrices have been claimed to add their own sources of error in an ISRM[22, 7]. Such as compressing ranges[7], *presumption of regular intervals* e.g. different people at different levels in an organization will rate scales differently[22], and *presumption of independence* between risks, some risks are more likely to happen together, and may together present a risk of higher magnitude[22].
Campbell[12] further critics scoring methods that multiplies results, and states that a high-impact low-probability risk is not the same as a high-probability low-impact risk.
There also exist methods that have moved away from using probabilities/likelihood, there exists critique of this as the method no longer is a forecasting method, and cannot be used for *”prediction of probable consequences of action”*[22].
Shedden et. al.[31] comments that traditional checklist-based methods have a too generic and limited perspective, and that they fail at effectively tying the assessment method to the business. She also claims that established ISRM methods have limitations in viewing people as assets, by not making the distinction between protecting the person and the knowledge.

Lack of Empirical Research and Good Data
Hubbard[22] state that if RM worked the way it was supposed to, a RM program would provide better IS and regulatory compliance records than companies in their peer groups that lack such programs. There would be a clear difference in performance, but there exists no valid evidence to support that ISRM improves corporate performance[22].
Gregory[16] claims that threat forecasting data is sparse, that there is a lack of data on the topic of cyber-related risk, and a lack of understanding of the existing data from a statistical perspective.

Level 3, Context Establishment

Lack of Validation and Testing
Zhiwei[42] points to a lack of analysis and judgment to the overall development tendency of risk evaluation. While Hubbard[22] claim that component testing and completeness checks are virtually non-existent in ISRM methodologies.

Organizational Disconnect
Jaquith[24] claims that viewing security as a product and not a process causes organizational disconnect in spending. He elaborates that spending money on independent security products outside of organizational context is not likely improve security. This view is further strengthened by Zhiwei[42] who claims that risk evaluation methodologies

"fail to take function and goal of information systems in the organization into consideration, which indicates that the basic problem of why to carry on risk evaluation has not been solved"[42]. Zhiwei further claims that safeguarding information should not be the main target of information security it should be to guarantee the reliability and security in the operational processes and goals in the organization.
Ozkan and Karabacak[28] points to the lack of knowledge from IS/IT professionals regarding the intersection between business and IT processes as being a problem, a risk assessment will lack completeness and produce erroneous results if the practitioners do not have a firm grasp of the business processes.
Another cause for organizational disconnect in ISRM mentioned by Ozkan and Karabacak[28] is when the IT-department are being the drivers and doers of ISRM and ISMS work. *Not realizing that information security is a corporate governance responsibility* is also coined as one of the ten deadly sins of IS[40].

Level 3, Risk Communication

Risk Vocabulary

There are several examples of ISRM professionals not speaking the same "language", a quick look at ISRM standards and frameworks reveal that many use their own definitions of risk [24]. One example of this provided by Hubbard[22] is the definition where risk can be perceived as a good thing; Hubbard claims that the positive outcomes from risks are covered by uncertainty (which is also a word that holds different meaning to different people[22]). In contradiction to Hubbard, David Hillson[20] argues that the common usage of the word *risk* sees only downside. Risk is according to Hillson *the uncertainty that matters*, and adds additional risk treatment strategies for handling "opportunity risks". Lack of a common language for IS risk professionals is a major factor that slows down progression within the research field[22, 2, 15].
There also seems to be some confusion regarding the terms "probability" and "likelihood", some standards use these terms interchangeably[23, 4], while there are other instances where likelihood represent the softer subjective approaches and probability represents quantitative numbers[26].
Interpretation of subjective wording is Another source of confusion pointed to by Campbell[12]. An example of this is one persons "trivial" injury can be another persons "minor" injury, this problem is also mentioned by Hubbard and Harris[22, 18].

Level 3, Risk Treatment

Biased Treatment Strategy

According to Blakley et. al.[10], risk treatment strategies applied in IS primarily focus on risk mitigation. Transference, acceptance and avoidance are alternatives that are seldom considered. The authors further claim that IS as a discipline focus more on reducing the probability of an event than on reducing its consequences.

Level 3, Risk Acceptance

Biased Decision Making

Hubbard[22] points to mistakes in making the assumption that the decision maker is "risk

neutral", when few or no people are truly risk neutral, and further claims that how much a decision maker values a risk depends on his/hers risk aversion.

Level 3, Risk Monitoring and Review

Lack of Validation and Measuring

Campbell[12] questions the credibility of subjective/qualitative risk assessments. While Hubbard[22] goes further and claim that new qualitative RM/RA methods do not work. Hubbard claims that RA/RM methods do not account for all the sources of errors in an organization, and some even add their own error, and states: *"Except for certain quantitative methods in certain industries, the effectiveness of risk management is almost never measured"*[22]. Hubbard further points to the lack of objective measurements of risk and validation of RM programs, together with the lack of confirmation of a program really works or not.

Level 4, Risk Identification

Assets

Both Ozkan et.al.[28] and Jaquith[24] point to asset evaluation as a challenge. Putting monetary value on something such as an intangible asset presents a major difficulty, as assets are often dynamic entities that change regularly. However, failing to recognize intangible assets in a RA will cause the assessment to be incomplete as they represents the social and non-technical dimension in an organization. Shedden et. al.[31] make a similar point regarding assets and claim that the current view of ISRM is too technical when it comes to assets. She also points to the problem that the view one takes on assets will affect the risk profile of assessed organization.
Zhiwei[42] critiques the asset-based approach by claiming that protection of assets is not a primary goal of organizations, and claims that protection of the reliability and security in the organization's business processes should be the main goal of IS.

Missing important risks

The current practice of ISRM evaluates each risk on its own and therefore misses correlations between risks states Hubbard[22], e.g. two or more risk events being tied together and creating a domino effect when one risk materializes , and calls this "Cascading risk". Hubbard also explains another concept he claims current RM misses, "Common Mode failure", is when one risk damages more than one system at a time. Hole and Netland[21] claims that traditional ISRM methods underestimate the risks of large-impact, hard-to-predict, and rare events in information systems, so called "Black Swans".

Level 4, Risk Estimation

Lack of Empirical Research and Good Data

Blakley et.al.[10] suggest a connection between a rapid increase in threats and vulnerabilities and a constantly evolving threat picture leading to lack of quality historical data and difficulties in quantitative data collection.

Qualitative Risk Analysis

Several authors claim that the applied qualitative methods are often untested, and we have little knowledge about the effectiveness of the controls we implement to mitigate risk[18, 22, 10]. Harris[18] states that the Qualitative risk assessments and its results are subjective and opinion-based, and involves a high degree of guesswork.

The subjective values eliminates the opportunity to create a dollar value for cost/benefit discussions, which makes it hard to develop a security budget from the RA results[18]. Because of the lack of standardization, each vendor has its own way of interpreting the qualitative processes and their results[18].

The dependence of expert predictions for the qualitative ISRA makes risk estimates for security events unreliable and opens for abuse of the ISRA to fit one's own agenda[9]. Another point of criticism of applying the expert prediction is that it has been proven that people are generally not well calibrated to estimate probabilities[30, 22, 34, 33]. Another criticism of the subjective likelihood scale is that Campbell[12] claim that there is no way of telling the relationship between numbers once it has been converted into the subjective scale.

Quantitative Risk Analysis

Several authors[18, 28, 37] claim that trying to use mathematical formulas for the calculation of risk is confusing, too much work, complex, time consuming and that it requires more preliminary work. Gregory[16] state that the reason for this is that it can be difficult to ascertain reasonable probabilities of threats and their financial impact, and reserves the usage of this method for the highest risk areas. Harris[18] claims that there exists misconceptions about quantitative analysis being purely objective and scientific, and state that it is hard to avoid some degree of subjectivity when it comes the data. Harris further claim that there is no standardized approach to quantitative ISRA, and that each vendor has its own way of interpreting the processes and their results.

There is also criticism claiming that the current quantitative ISRA methods misses the point by not addressing how to calculate probability[26, 29]. They claim that the general description of quantitative ISRA methods are either as SLE or ALE (single and annual loss expectancy) or both, both of which are dependent on probabilities, but they do not address how to calculate the probability itself. Several other sources also point to the difficulty of calculating probabilities without having quality historical data available[9, 39, 27, 16].

Risk Perception

Loewenstein et.al[27] explains how risk analysts are affected by their feelings when analyzing a risk. It has also been proven that risk is perceived differently by genders and races[19], and that different people at different levels in the organizations perceive risk differently[25]. Hubbard[22] claims that subjective risk perceptions are also victim to certain aspects of human nature. Such as the tendency of being overconfident in ones own estimates, and human experts also, tend to make consistent types of errors in judgments about uncertainty and risk, such as underestimating risk. People can also develop tolerance to serious risks after experiencing near misses on several occasions[22]. Peoples ability to estimate is also inconsistent[22].

"Framing" is a concept that illustrates that the way people are asked a question affects how they answer it[38]. This also applies to risk management[22, 35], where framing of a risk might bias the decision maker.

Level 4, Risk Evaluation

ALE (Annual Loss Expectancy) and SLE (Single Loss Expectancy) Criticism
There exists several points of criticism to ALE and SLE. Jaquith[24] claims that ALE does not work and presents several problems with the approach: The inherent difficulty in modeling outliers, and it is difficult to model a typical loss event. Another reason is *"the lack of data for estimating probabilities of occurrence or loss expectancies, and the sensitivity of the ALE model to small changes in assumptions"*[24]. The author further claims that using averages adds error because real events tend to cluster at the extremes of the scale.
ALE and SLE reduces risk into a single number (vector), by multiplying them together. This does not allow for ranges e.g. for losses (as damage from a fire might result in various losses). Risk is both the probability and the consequence, and should be represented as multiple vectors[22].
Ekelhart [14] comments that the concrete calculation of ALE is dependent on expensive expert knowledge, which is not available to small and medium sized enterprises. Ekelhart also comments on the complexity of the ALE calculation, which can be very high, but is still likely to be dependent on subjective probabilities.
Schetcher[29] claims that ALE does not specify how to forecast either loss events that will occur or reductions in rates that will result from adding safe guards.

4 Analysis and Discussion

In this section we analyze and discuss the findings from chapter 3 to obtain an understanding of the most prevalent causes of problems within ISRM.
One of the biggest problems identified in the existing ISRM literature is the lack of validation and verification of existing methods. This problem occurred in much of the visited literature and at different levels in the taxonomy. The qualitative methods and ALE/SLE were especially targets for this criticism. It is our opinion that being able to validate and verify if a method works would represent a huge leap in ISRM by putting a nail in the coffin for many of these discussions. In relation to this, although not mentioned in our taxonomy, we observed that none of the existing taxonomies we visited sorted ISRM methods on proven performance, such as measurable improvements in organizations. Related to the previous problem is the lack of empirical research and good data within IS. The reason for this is explained by Kotulic[25], and is still a major obstacle that need to be overcome to be able to make progress.
There must be tools available for IS professionals to be able to perform quantitative risk analysis; the literature points to a gap when it comes to explaining quantitative methods, referring to ALE/SLE and historical data as the quantitative approaches to ISRA. However, this presents a problem when there are apparent difficulties in calculating probabilities for ALE/SLE and little historical data available. There has been made attempts at solving the likelihood and probabilities problem by removing probabilities or making them optional, e.g. OCTAVE[5]. This introduces a new problem; without probabilities, we are no longer forecasting events. Can one conduct a meaningful risk analysis without addressing probability of an event occurring, and how does one address uncertainty without probabilities?
Although few ISRM methods mention "cascading risks" and "common mode failures", "Failure mode and effect analysis" is a RA method that exists to address complex risks

such as these. However, we do not know how popular this method is.
The misconception that ISRM is mainly an IT activity was a problem in 2001[10], and still is in 2013[18]. This knowledge gap seems therefore to be a prevalent cause for problems in ISRM. Viewing ISRM as a purely technical discipline, has among other things the potential of preventing human factors from being risk analyzed, disregarding intangible assets, and causing organizational disconnect in both managing risks and spending.
It is likely that many of the misconceptions about ISRM stem from the lack of a common IS and risk vocabulary. An example of this is the many definitions of the word *risk*. This creates an obstacle for progression within IS, as professionals from different RM fields must first come to an agreement of what a risk is, before having a meaningful discussion on the topic.
There are several factors adding ambiguity to the ISRM process, and risk perception seem to be a prevalent problem. A large amount of literature points to people generally being bad at estimating risk: gender, age, race, emotional state, organizational rank, framing, etc all affect how we perceive risk. It is unlikely that two people will rate a particular risk the same, and in addition to being susceptible to all of the above, subject experts tend to underestimate risk and show overconfidence in their own estimates. Related to both the risk vocabulary and perception is using subjective words to define risk likelihood and severity. The interpretation of the chance of a ”high” probability risk occurring is likely to differ within an organization, compressing probability ranges to fit in risk matrices, and multiplication of results all add their own potential sources of error.

5 Conclusion

The cornerstone of IS, ISRM, is a field with many challenges due to the complexity of the field. Managing risk will never be an exact science and there will always be uncertainty when forecasting is involved. However, we have shown in this article that there is much room for improvement. We have presented a taxonomy based traditional ISRM activities, for the purpose of classification of challenges within the ISRM research field. We have also provided a non-exhaustive backlog of challenges that exist within the research field, and classified it within the taxonomy. We have also identified a collection of important challenges that are prevalent in ISRM, and provided a foundation for a holistic understanding of underlying causes of problems.

References

[1] Enisa, inventory of risk assessment and risk management methods. Technical report, 2006.

[2] Risk taxonomy. Technical report, The Open Group, 2013.

[3] Information technology, security techniques, isms, overview and vocabulary, ISO/IEC 27000:2009.

[4] Information technology, security techniques, information security risk management, ISO/IEC 27005:2011.

[5] Christopher J Alberts and Audrey J Dorofee. *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003.

[6] Ross Anderson. Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pages 358–365. IEEE, 2001.

[7] Louis Anthony Tony Cox. What's wrong with risk matrices? *Risk analysis*, 28(2):497–512, 2008.

[8] Behnia, Rashid, and Chaudry. A survey of information secuirty risk analysis methods. *Smart Computing Review*, 2(1), 2012.

[9] Vicki M. Bier. Challenges to the acceptance of probabilistic risk analysis. *Risk Analysis*, 19(4):703–710, 1999.

[10] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms*, pages 97–104. ACM, 2001.

[11] WG Bornman and L Labuschagne. A comparative framework for evaluating information security risk management methods. In *Information Security South Africa Conference*, 2004.

[12] Harry Campbell. Risk assessment: subjective or objective? *Engineering Science and Education Journal*, 7(2):57–63, 1998.

[13] Philip L. Campbell and Jason E. Stamp. *A classification scheme for risk assessment methods*. Sandia National Laboratories, 2004.

[14] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, pages 1–10, 2009.

[15] Andreas Ekelhart, Stefan Fenz, Markus Klemen, and Edgar Weippl. Security ontologies: Improving quantitative risk analysis. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 156a–156a. IEEE, 2007.

[16] Peter H. Gregory. *All in one - CISA - Certified Information Systems Auditor - Exam Guide*. McGraw-Hill Companies, 2012.

[17] J. Hagen. Human relationships: A never-ending security education challenge? *Security Privacy, IEEE*, 7(4):65–67, 2009.

[18] Shon Harris. All in one cissp. *USA: MacGraw Hill*, 2013.

[19] Joni Hersch. Smoking, seat belts, and other risky consumer decisions: Differences by gender and race. *Managerial and Decision Economics*, 17(5):471–481, 1996.

[20] David Hilson. Extending the risk process to manage opportunities. *International Journal of Project Management*, 20(3):235–240, 2002.

[21] Kjell J Hole and L-H Netland. Toward risk assessment of large-impact and rare events. *Security & Privacy, IEEE*, 8(3):21–27, 2010.

[22] Douglas W Hubbard. *The failure of risk management: Why it's broken and how to fix it*. Wiley, 2009.

[23] ISACA. The risk it framework. Technical report, 2009.

[24] Andrew Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Upper Saddle River, 2007.

[25] Andrew G Kotulic and Jan Guynes Clark. Why there arent more information security research studies. *Information & Management*, 41(5):597–607, 2004.

[26] Douglas J Landoll. *The security risk assessment handbook*. CRC Press, 2005.

[27] George F Loewenstein, Elke U Weber, Christopher K Hsee, and Ned Welch. Risk as feelings. *Psychological bulletin*, 127(2):267, 2001.

[28] Sevgi Ozkan and Bilge Karabacak. Collaborative risk method for ism practices: A case context within turkey. *International Journal of Information Management*, 30(6):567–572, 2010.

[29] Stuart Edward Schechter. *Computer security strength & risk: A quantitative approach*. PhD thesis, Citeseer, 2004.

[30] James Shanteau and Thomas R. Stewart. Why study expert decision making? some historical perspectives and comments. *Organizational Behavior and Human Decision Processes*, 53(2), 1992.

[31] Piya Shedden, Wally Smith, and Atif Ahmad. Information security risk assessment: towards a business practice perspective. In *Australian Information Security Management Conference*. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2010.

[32] Mikko T Siponen and Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *ACM Sigmis Database*, 38(1):60–80, 2007.

[33] Paul Slovic. Perception of risk. *Science*, 236(4799):280–285, 1987.

[34] Paul Slovic, Melissa L Finucane, Ellen Peters, and Donald G MacGregor. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, 24(2):311–322, 2004.

[35] Einar Snekkenes. An information security risk management research menu. *Norsk informasjonssikkerhetskonferanse (NISK)*, 2012, 2012.

[36] Amril Syalim, Yoshiki Hori, Kouchi, and Kouchi Sakurai. Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide. *International Conference on Availability, Reliability and Security*, pages 726–731, 2009.

[37] Carrison KS Tong, KH Fung, Henry YH Huang, and Kwok Kwan Chan. Implementation of iso17799 and bs7799 in picture archiving and communication system: local experience in implementation of bs7799 standard. In *International Congress Series*, volume 1256, pages 311–318. Elsevier, 2003.

[38] Amos Tversky, D Kahneman, and Rational Choice. The framing of decisions. *Science*, 211:453–458, 1981.

[39] Amos Tversky and Daniel Kahneman. Judgment under uncertainty: Heuristics and biases. In Dirk Wendt and Charles Vlek, editors, *Utility, Probability, and Human Decision Making*, volume 11 of *Theory and Decision Library*, pages 141–162. Springer Netherlands, 1975.

[40] Basie Von Solms and Rossouw Von Solms. The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376, 2004.

[41] H.J. Whitman, M.E. & Mattord. *Roadmap to information Security: For IT and InfoSec Managers*. Cengage Learning, 2011.

[42] Yu Zhiwei and Ji Zhongyuan. A survey on the evolution of risk evaluation for information systems security. *Energy Procedia*, 17:1288–1294, 2012.