Proceedings of the Federated Conference on Computer Science and Information Systems pp. 999–1008
DOI: 10.15439/2016F158
ACSIS, Vol. 8. ISSN 2300-5963

An initial insight into Information Security Risk Assessment practices

Gaute Wangen
NISLab and CCIS, NTNU Gjovik
Teknologiveien 22, 2802 Gjovik, Norway
Email: gaute.wangen2@ntnu.no

***Abstract*—Much of the debate surrounding risk management in information security (InfoSec) has been at the academic level, where the question of how practitioners view predominant issues is an essential element often left unexplored. Thus, this article represents an initial insight into how the InfoSec risk professionals see the InfoSec risk assessment (ISRA) field. We present the results of a 46-participant study where have gathered data regarding known issues in ISRA. The survey design was such that we collected both qualitative and quantitative data for analysis. One of the key contributions from the study is knowledge regarding how to handle risks at different organizational tiers, together with an insight into key roles and knowledge needed to conduct risk assessments. Also, we document several issues concerning the application of qualitative and quantitative methods, together with drawbacks and advantages. The findings of the analysis provides incentives to strengthen the research and scientific work for future research in InfoSec management.**

I. Introduction

THE PRIMARY goal of InfoSec is to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity, availability, and non-repudiation [1]. Best practice InfoSec is highly dependent on well-functioning InfoSec risk management (ISRM) processes[2]. While ISRM is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve acceptance[3].

This paper investigates the practitioners view of research problems within information security (InfoSec) risk assessment (ISRA). While there is plenty of available material regarding what ISRA frameworks contain and how they compare with each other [4], the literature is scarce regarding the current ISRA industry practices. There are several known theoretical problems in ISRA[4], [5], however, we do not know if the risk practitioners agree that these problems are either relevant or representative. Thus, there is the possibility that existing literature is incomplete and that academia is missing the important issues. This paper contains the results and analysis from a combined quantitative and qualitative study of the practitioners view, and represents a step towards a more holistic picture of industry ISRA practices.

Part one of this study [6] researched practices in InfoSec (ISRM) with emphasis on the risk management part and issues, while this study emphasizes the risk assessment and analysis parts. We provide new knowledge regarding where the research in ISRA should be focusing the efforts, making the ISRA community and researchers the primary beneficiaries of this study. Improving ISRA is essential in making progress in the InfoSec research field as it is this process that helps organizations determine what and how to protect. Thus, the intended audience of this paper is InfoSec professionals and academics, together with other ISRA practitioners and stakeholders.

The main research problem investigated in this article is "How do the ISRA problems outlined in previous work ([4]) reflect problems experienced in the industry?". The scope of this article covers the ISRA process, including risk identification, estimation, evaluation, and risk treatment practices [3], and is limited to the practitioner point-of-view. We separate between risk assessment (ISRA) and analysis (ISRAn), where the assessment is defined as the overall process of risk identification, estimation, and evaluation. While risk analysis is the practical hands-on parts of risk identification and estimation, for example, a practitioner may choose ISO/IEC 27005:2011 as the overall approach to ISRM/ISRA, while prioritizing *Fault tree analysis* for ISRAn.

The remainder of this article has the following structure: First, we briefly describe the related work, before presenting the research method in the form of data collection approach, demographics, and analysis. Following this is a combined analysis and discussion of the results, where we start with findings on the high-level risk assessment practices, before diving into the deeper aspects of InfoSec risk analysis (ISRAn) and risk treatment. Lastly, we summarize our findings, including limitations of this study, and conclude the paper.

A. Related work

This work primarily builds on previous work conducted on the topic of research problems in ISRM/ISRA. Both Wangen and Snekkenes [4] and Fenz et al. [5] have published articles on current challenges in ISRM; The former is a literature review that categorizes research problems into a taxonomy. The latter discusses current challenges in ISRM, pre-defines a set of research challenges, and compares how the existing ISRM methods support them. The primary purpose of the Fenz et al. study was to categorize and present known research problems at different stages in the ISRM/RA areas and activities. These two articles provide the primary literature foundation for this study. The data for this study was gathered in one comprehensive questionnaire, where the first part concerning ISRM was published in [6].

II. Research Method

This study was conducted to investigate ISRM industry practices and the respondents' views of several known challenges within the research field. 46 respondents participated in

Fig. 1. How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)

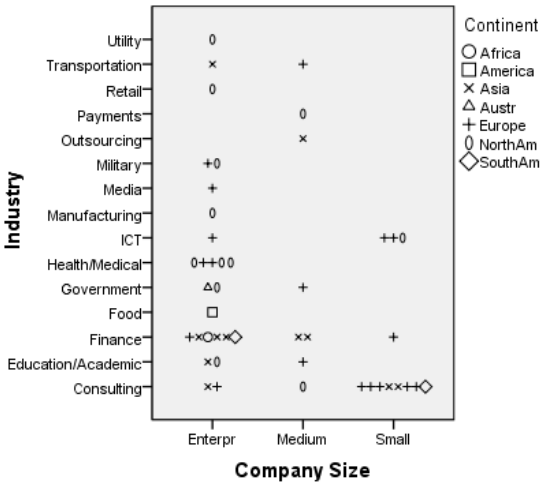

Fig. 2. Respondent demographics, based on company size (x-axis), industry (Y-axis) and Continent.

our online survey. The first sub-section addresses the choice of data collection method and measurement, followed by the demographics, and a brief overview of the statistical methods used for data analysis.

A. Data Collection, Sample, and Measurement

In their study, Kotulic and Clark [7] highlights that one of the most prominent problems in InfoSec studies is getting in touch with the target group and acquiring respondents. They propose several potential explanation for this: Where one is that InfoSec research is one of the most intrusive types of organizational studies. Also, that there is a general mistrust of any ”outsider” attempting to gain data about the actions of the security practitioner community [7]. Thus, we consider non-intrusiveness an essential requirement when designing the data collection tool. The narrow target group, industry professionals, made obtaining respondents a challenge as the study was subject to geographical limitations. To overcome said limitations we attempted to recruit participants from InfoSec risk specialized online forums. We considered this approach as non-intrusive, and it exposed the survey to many within the target group. However, it presents several problems; with this strategy the researcher has little control of participants except that they are members of particular forums, Table I. We, therefore, included self-rating questions in the questionnaire for the respondents to rate their knowledge, expertise and experience, together with our knowledge-based control questions. We designed a classification scheme based on this information, see Fig. 1.

We designed the questionnaire in Google Forms according to the procedure for developing better measures [8]. As for the level of measurement, the questionnaire had category, ordinal, and continuous type questions. Category type questions mainly for demographics and categorical analysis, while the main bulk of questions were designed using several mandatory scale- and ranking questions. The main categories applied for analysis is seen in Fig. 1, together with company size, and work type. The questionnaire also included several non-mandatory fields for commenting on previous questions or just for sharing knowledge about a subject. It had four pages of questions in total; the first page was demographics and self-rating questions. The questionnaire consisted of 37 questions in total, with an estimated completion time of 15-40 minutes depending on how much information the respondent shared. This paper consists of the results from questions regarding risk assessment and analysis.

TABLE I. GROUPS AND FORUMS WHERE THE QUESTIONNAIRE WAS POSTED

LinkedIN Forum name	**Members (at release time)**
IT Risk Management	3 443
CRISC (Official) *(Certified in Risk and Information Systems Control)*	1 400
Information Security Risk Assessment	441
ISO27000 for Information Security Management	22 620
Information Security Expert Center	8 906
Risk Management & Information Security *(Google+)*	521

B. Demographics

We received 46 accepted answers, See Table II for the classification of respondent expertise and work type (technical or administrative). While Fig. 2 displays respondent demographics categorized on company size, industry, and geographical affiliation. For the analysis, we applied the following definitions of company size: Small equals 1-249 employees, Medium 250 -1000, and Enterprise more than 1000.

TABLE II. CLASSIFICATION OF RESPONDENTS, TOTAL 46.

	Expert	Proficient	Competent
Administrative Work	13	10	6
Technical Work	7	7	3

C. Analysis

We applied a variety of statistical data analysis methods specified in the results, and the IBM SPSS software for the statistical analysis. A summary of the statistical tests used in this research is as follows:

For *Descriptive analysis* we have considered distributions including range and standard deviation. On continuous type

questions, we applied measures of central tendency mean, median and mode. We also conducted *Univariate* analysis of individual issues, and *Bivariate* analysis for pairs of questions, such as a category and a continuous question, to see how they compare and interact. However, we have restricted the use of mean and standard deviation for Likert-type questions and ordinal data where there was not defined a clear scale of measurement between the alternatives, as the collected data will seldom satisfy the requirements of normality. We have, therefore, analyzed the median together with an analysis of range, minimum and maximum values, and variance. This study also analyses the distributions of the answers, for example, if they are normal, uniform, binomial, or similar. *Crosstabulation* was applied to analyze the association between two category type questions, such as "Company Size" and "Expertise." We have used Pearson two-tailed *Correlation test* to reveal relationships between pairs of variables as this test does not assume normality in the sample.

The questionnaire also had several open-ended questions. We have treated these by listing and categorizing the responses. Further, we counted the occurrence of each theme and summarized the responses. Also, each continuous question had the possibility for the respondent to write a comment and offer further qualitative insight on an issue, where the most valuable comments are a part of this paper.

III. InfoSec Risk Assessment practices

This section contains the results and discussion of the statistical analysis regarding the ISRA practices. We start at a high-level; with the ISRA practices in organizational tiers, who should attend the ISRA, and what knowledge is important to have included in the process.

A. ISRA and Organizational Tiers

It is common to differentiate between risks at different tiers of abstraction when assessing an organization, such as Operational/Information Systems (low level), Tactical (mid-level), and Strategic (high level) information risks (for example [9]). The strategic and tactical type-risks can provide the risk analyst more time to estimate, risks in the operational environment often has to be handled ad-hoc or within a limited period. As these tiers are quite different and come with different types of risk, we asked if the practitioners distinguish between ISRA methods for them. 28% answered that they do, while the remainder answered no or other. There was no significant difference between groups in this question, Fig. 3. There were three detailed technical insights offered by the participants to shed light on practices, one technical (tech) expert responded: *"We apply the same methodology but are far less formal with tactical solutions. While a strategic solution would require formal sign off, tactical solutions need only require an email approval."*

While an administrative (admin) expert answered:*"High or Very High risks require detailed documented analysis (eg Bowtie diagrams) At each organisational level the risks are assessed against consequences at that level and mitigation applied at that level - if mitigation are insufficient at that level, the risk is escalated to the next higher level and re-assessed."*

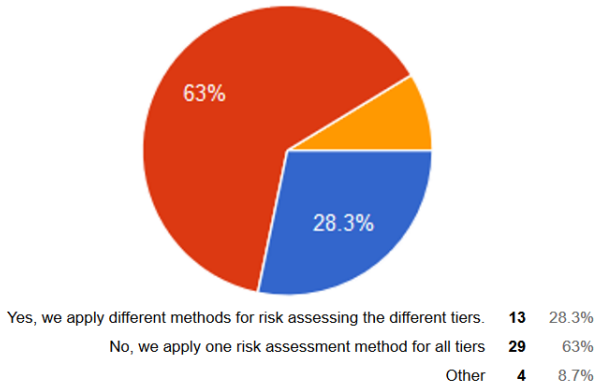

Fig. 3. ISRA practices on different organizational tiers

A tech proficient respondent answered: *"We use different methods for financial risk, IT (security) risk and business strategic risk. method for financial risk is "FOCUS" (successor of "FIRM"), as prescribed in regulations; method for IT security risk based on ISO 27005/31000, method for strategic risk is not formalised."*

The three answers show that there are several nuances to this problem that has not yet been highlighted in academia. The lower organizational tiers may be handled less informally, as it is likely these need faster decision-making. Our results show that some organizations have implemented different approaches to dealing with this problem, while others stick to one approach for all risk types. Awareness around this issue is also something that can be further researched in academia.

B. Who attends and conducts InfoSec risk assessments?

Having people with the right expertise and knowledge about the target system attending the risk assessment is one crucial success factor. Our results should provide a pointer on how to organize thee risk assessment and who should attend.

To get a generic overview of who attends and conducts ISRA in the practitioners organizations, we asked the participants who attends risk assessments in their organization. As two respondents pointed out, this picture depends on the type of risk assessment being conducted, yet, frequencies of attendance can still be estimated. Table III holds an overview of who attends ISRAs in the respondents organizations. The alternatives was "Never attends" (1), Sometimes attends (2), Always attends (3), Leads assessments (4), and we removed the respondents opting *Not present* for the statistical analysis, Table IV.

The results show that the CSO/CISO (Chief InfoSec Officer) most frequently leads risk assessments, while ICT security personnel most frequently attends. With the Head of ICT department and Operations personnel also attending with a high frequency. IT architects and software developers also attend the ISRA process frequently.

We found that in smaller companies, the CEO and CTO is much more likely to attend/lead risk assessments than in medium and enterprise sized companies, Table IV. Although, in some organizations, especially small ones, employees will have overlapping roles. One admin expert provided a caveat

about having high management involved: *"Having C[EO] or high management inside Information Security assessment will not allow the participants to be open when providing input for risk identification."*[1]

Comments on the results in table III, were from six admin experts and one admin proficient. Out of the seven written comments, five of them specified that the composition of the risk assessment team is dependent on the scope of the assessment; *"If business processes or systems are included in the scope, system owners or users with good knowledge of the processes attend."*

TABLE III. ROLES ATTENDING IN RISK ASSESSMENTS.

Attends/ Roles	Never present	Sometimes	Always	Leads	Not present in Organiza.
CEO	34.8%	28.3%	15.2%	13 %	8.7%
CSO/CISO	4.3%	15.2%	34.8%	32.6%	13 %
CTO	15.2%	17.4%	30.4%	8.7%	28.3%
CIO	19.6%	19.6%	28.3%	13 %	19.6%
Head of IT Dep	10.9%	26.1%	32.6%	21.7%	8.7%
ICT sec. personnel	4.3%	8.7%	50 %	30.4%	6.5%
IT architects	8.7%	34.8%	30.4%	13%	13%
Softw. dev	8.7%	39.1%	30.4%	10.9%	10.9%
Operations Personnel	8.7%	32.6%	37 %	15.2%	6.5%
External Consultants	21.7%	43.5%	15.2%	6.5%	13 %

TABLE IV. NOTICEABLE DIFFERENCES BETWEEN ATTENDS, SCALE FROM 1 (NEVER ATTENDS) - 4 (ALWAYS ATTENDS). (NOTE: THE RESPONDENTS CHOOSING "NOT PRESENT IN ORG." HAS BEEN REMOVED FROM THE SAMPLE)

		N	Minimum	Maximum	Range	Median	Grouped Median
@CEO	Small	12	0	4	4	3,00	2,67
	Medium	8	1	4	3	2,00	1,71
	Enterpr	26	0	4	4	1,00	1,53
CTO	Small	12	0	4	4	3,00	2,10
	Medium	8	0	4	4	2,00	2,00
	Enterpr	26	0	4	4	2,00	1,69

C. Critical knowledge areas in ISRA

Conducting an ISRA is a complex task with several different variables to consider, having discussed who attends risk assessments we look into critical knowledge areas to succeed with a risk assessment. So, we asked the participants to rank the importance of having knowledge about a set of items for the results of the ISRA (scale: 1 equals "not important" - 6 "very important"), Table V. For the comparison of knowledge areas the median is 5 for all but the *Organizational Structure* option, meaning that all were ranked highly by the respondents. Knowledge of *information assets* as the most important according to the mean score. Second, knowledge about *Laws & regulations* and *Information systems* were ranked equally, knowledge about *ISRA methods* was ranked the lowest. The diversity of the alternatives and the density of the results, supports that InfoSec is a very diverse field which demands a broad range of knowledge form its practitioners.

There was three noticeable differences between the expertise categories, the difference in view between experts and the two other groups on the importance of software, threat intelligence, and ISRA methods, Table VI. Whereas the experts valued threat intelligence less (grouped median = 4.75) than the proficient and the competent (grouped median = 5.13 and 5.47). There was also a slight difference in views between administrative (median=5, grouped median = 4.71) and technical workers (median=4, grouped median=4.71) on having knowledge of the organizational structure.

Two experts commented on the criticality of experience, *"The assessors experience is critical to a effective and accurate risk assessment"*, and *"Any method in use is only as good as the person(s) executing it and overall understanding of the business (or the part of business to evaluate) is critical to get results that are business beneficiary and useful to work with"*. Both comments highlights the need for experience, while the latter also highlights business understanding as key knowledge items. Our results also support this, as the top three ranked knowledge items relate to business understanding.

TABLE V. VIEWS ON IMPORTANCE OF KNOWLEDGE AREAS FOR ISRA. (*1 - Not Important* TO *6 - Very Important*

	1. Laws & Regulations	1. Info Assets	3. Info Systems	4. IT Infrastr & Hardware	5. Business Processes	6. Software
N	46	46	46	46	46	46
Min	2	3	3	3	1	3
Max	6	6	6	6	6	6
Median	5	5	5	5	5	5
Range	4	3	3	3	5	3
Mean	5,09	5,28	5,09	5,02	4,96	4,72
Std. Dev.	1,05	0,861	0,839	0,856	1,173	1,004
	7. Stakeholders & Employees	8. Organizat. Structure	9. ICT Architecture	10. Threat Intelligence	11. ISRA Methods	12. Pers. Expert & Experience
N	46	46	46	46	46	46
Min	1	2	3	2	1	3
Max	6	6	6	6	6	6
Median	5	4	5	5	5	5
Range	5	4	3	4	5	3
Mean	4,83	4,57	4,85	4,98	4,52	4,93
Std. Dev.	1,122	0,981	0,788	1	1,11	0,879

TABLE VI. NOTABLE DIFFERENCES ON KNOWLEDGE AREAS BETWEEN EXPERTISE GROUPS

		N	Min	Max	Range	Median	Grouped Median
Software	Competent	9	4	6	2	5,00	5,14
	Proficient	17	3	6	3	4,00	4,50
	Expert	20	3	6	3	4,50	4,67
Threat intel	Competent	9	4	6	2	5,00	5,13
	Proficient	17	2	6	4	6,00	5,47
	Expert	20	3	6	3	5,00	4,75
ISRA Methods	Competent	9	3	6	3	5,00	4,83
	Proficient	17	1	6	5	4,00	4,56
	Expert	20	3	6	3	5,00	4,50

IV. RISK ANALYSIS PRACTICES

Risk analysis (ISRAn) is the hands-on tasks performed during the assessment, primarily risk identification and estimation related tasks. This section starts with addressing some common issues regarding information assets, before investigating common risk analysis issues. We then survey the views of ISRAn methods and concepts.

We started the inquiry by asking an optional question on what the respondents thought to be working well in ISRAn. We got sixteen valid answers (eighteen total) with few common denominators, notably six respondents rated the risk assessment process to be working well, where two specified the risk identification phases to be well-developed. Two tech experts and one admin expert mentioned quantitative (numerical) ISRAn methods to be working well. While one tech and one admin expert answered that risk assessment on an overall works well, while *"implementation of risk mitigation and measurement follow up lags in many organizations."*

[1]Edited by author for readability, original answer *"having C or high management inside Information Security assessment not allow the participants to be open when providing input for risk identification."*

A. Views on Information Assets

Asset evaluation is one of the key challenges in ISRA [4], [10]. Due to being intangible, information assets can be particularly elusive to monetize and quantify. Which makes it hard to estimate, evaluate, and predict consequences of asset breaches in ISRA. To investigate issues regarding assets, we asked the participants to rate five statements regarding known issues on information assets [4]. Figure 4 shows the distribution of answers and Table VII displays descriptive statistics, typical of these results is a high variability in the answers.

With regards to Statement 1 (Table VII), the descriptives show that most practitioners agree that assigning monetary value is difficult, with the highest reported median 5 and mean 4.7, with no noticeable difference between groups. The results support the claims regarding information assets in Wangen & Snekkenes (2013) [4]).

The result from ranking Statement 2 regarding risk assessment method adequacy for asset evaluation, shows the sample mean being divided almost in the middle with a median of 3.67. The distribution for statement 2 is also close to normal but being negatively skewed (-0.299), Figure 4, and, therefore, ran significance tests. Our results showed that there was a statistically significant difference (P=0.031%) between expertise groups regarding Statement 2, regarding ISRA method adequacy, Table VIII, showing the Experts being less satisfied with the available asset value estimation methods. Three admin experts also commented on assigning the monetary value to assets, where two commented regarding asset evaluation not always being necessary: (i) *"The value doesn't necessarily be expressed in monetary terms."* (ii)*"... Knowing the value of personal information is not required to be able to protect it from unauthorized collection use of disclosure. The law says to do it."* These two insights show that asset evaluation is not always necessary, especially when the existing security legislation applies then a security classification is sufficient. While the third comment is on the importance of asset evaluation, (iii) *" Asset value can be assigned in various ways, and monetary value is in most cases the hardest one and most often wrongly set. Erroneously set values may in the worst case result in a totally erroneous assessment result. Asset value may have monetary value as one parameter but should be defined by much more than just a monetary number. E.g. if assets protected by law governed requirements are lost in the worst possible way, that may be "end of business," but that most often only relate to a small percentage of the total information assets of the business."*

Zhiwei [11] critiques the asset-based approach, and claims that protection of assets is not a primary goal of organizations, while priority number one should be the protection of the reliability and security of the organizations business processes. Statements 3 and 4 (Table VII addresses Zhiwei's view:

Regarding statement 3, most agreed that Asset protection is the primary goal of the InfoSec program, median = 5 and a mean = 4.37. However, there is a large variability in the results; nine respondents answered three or less showing that a minority disagrees with this statement. Out of this minority, six qualify as experts. The answer to statement 4 regarding the importance of asset security compared to ensuring stable

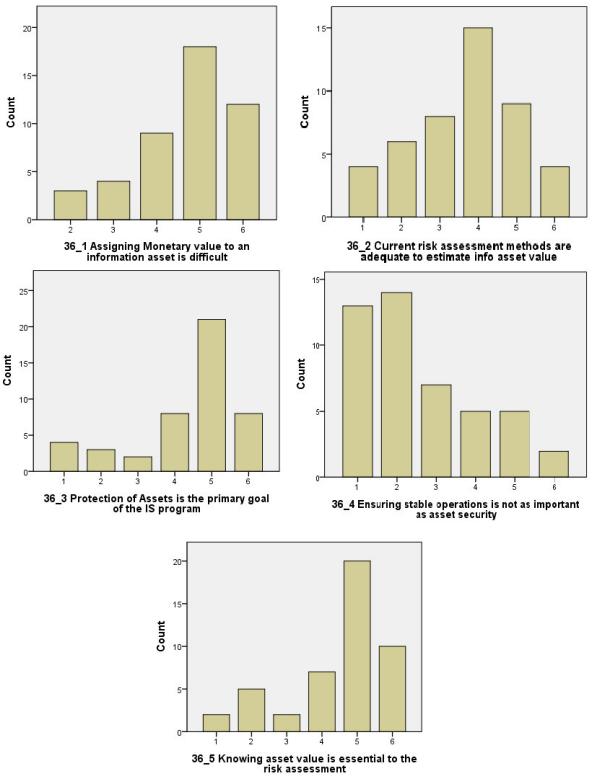

Fig. 4. Statements and rankings regarding Assets (Scale *1 - Strongly disagree* to *6 - Strongly agree*)

operations: The scores was on the low side (median = 2), showing that most of the respondents thought that stable operations are just as (or more) important than asset security. There was a notable difference between expertise groups for both Statement 3 and 4: The competent group consistently valued asset security higher than the proficient and expert group, indicating that protection priorities may be altered with experience in support of Zhiwei, Table VIII.

TABLE VII. PRACTITIONER VIEW ON ISSUES RELATED TO ASSETS. (SCALE 1 - STRONGLY DISAGREE, 6 - STRONGLY AGREE)

	N	Min	Max	Median	Range	Mean	Variance
1. Assigning Monetary value to an information asset is difficult	46	2	6	5	4	4,7	1,328
2. Current risk assessment methods are adequate to estimate info asset value	46	1	6	4	5	3,67	1,958
3. Protection of Assets is the primary goal of the IS program	46	1	6	5	5	4,37	2,149
4. Ensuring stable operations is not as important as asset security	46	1	6	2	5	2,59	2,248
5. Knowing asset value is essential to the risk assessment	46	1	6	5	5	4,48	1,988

TABLE VIII. STATISTICALLY SIGNIFICANT AND NOTABLE DIFFERENCES BETWEEN EXPERTISE CATEGORIES ON ASSETS

	Category	N	Mean	Std. Dev.	95% CI		Min	Max	
Asset Scenario					Lower Bound	Upper Bound			ANOVA, sig
2.	Competent	9	4,44	0,882	3,77	5,12	3	6	
	Proficient	17	3,94	1,298	3,27	4,61	2	6	
	Expert	20	3,1	1,483	2,41	3,79	1	6	
		46	3,67	1,399	3,26	4,09	1	6	.031
		9	Median	Range	Grouped Med				
4.	Competent	9	5	4	4.5		2	6	
	Proficient	17	2	5	1.92		1	6	
	Expert	20	2	3	2		1	4	
		46	2	5	2.29		1	6	

B. Views on common Risk Analysis issues

TABLE IX. DESCRIPTIVE STATISTICS OF ISRA STATEMENTS. (1 - STRONGLY DISAGREE, 6 - STRONGLY AGREE)

	N	Min	Max	Mean	Variance	Median	Skewness	Range
S1.Our ISRAn Methods are mainly Qualitative	46	2	6	4,41	1,537	5	-,414	4
S2.Our ISRAn Methods are mainly Quantitative/Statistical	46	1	6	3,26	2,597	3	,254	5
S3.It is easy to use the ISRAn results to predict the monetary cost of an incident	46	1	6	3,13	2,338	3	,161	5
S4.Our ISRAn method relies heavily on the security expert's predictions	46	1	6	3,87	1,405	4	-,574	5
S5.The resources spent on quantitative/statistical approaches are not worth the results	46	1	6	3,33	1,614	3	,472	5
S6.We find lack of historical data a problem for our risk forecasts/ predictions	46	1	6	4,17	1,614	4	-,341	5
S7.We lack a reliable method for mathematical ISRAn probability calculations	46	1	6	3,74	2,197	3	,087	5
S8.Annual Loss Expectation (ALE) is our preferred approach to calculating impact.	46	1	6	3,02	2,2	3	,474	5
S9.Our consequence/impact estimates of incidents tend to be precise	46	1	6	3,24	1,653	3	,252	5
S10.Consequences of occurred incidents tend to be outliers (extreme)	46	1	6	2,91	1,548	3	,316	5
S11.Causes for severe incidents/ disasters tend to not be thought of in our assessments	46	1	6	2,85	2,043	3	,518	5

TABLE X. DISTRIBUTION OF ANSWERS (X-AXIS) REGARDING ISRA STATEMENTS (Y-AXIS). STATEMENT NUMBERS CORRELATE WITH DESCRIPTIONS IN TABLE IX. (1 - STRONGLY DISAGREE, 6 - STRONGLY AGREE)

Statement nr	1	2	3	4	5	6
S1	0 (0%)	4 (8.7%)	7 (15.2%)	11 (23.9%)	14 (30.4%)	10 (21.7%)
S2	7 (15.2%)	10 (21.7%)	11 (23.9%)	5 (10.9%)	8 (17,4%)	5 (10.9%)
S3	8 (17.4%)	10 (21.7%)	10 (21.7%)	6 (13%)	10 (21.7%)	2 (4.3%)
S4	2 (4.3%)	3 (6.5%)	13 (28.3%)	10 (21.7%)	17 (37%)	1 (2.2%)
S5	2 (4.3%)	10 (21.7%)	18 (39.1%)	6 (13%)	7 (15.2%)	3 (6.5%)
S6	1 (2.2%)	3 (6.5%)	11 (23.9%)	10 (21.7%)	14 (30.4%)	7 (15.2%)
S7	2 (4.3%)	8 (17.4%)	14 (30.4%)	5 (10.9%)	10 (21.7%)	7 (15.2%)
S8	7 (15.2%)	12 (26.1%)	13 (28.3%)	4 (8.7%)	7 (15.2%)	3 (6.5%)
S9	4 (8.7%)	8 (17.4%)	18 (39.1%)	7 (15.2%)	7 (15.2%)	2 (4.3%)
S10	7 (15.2%)	8 (17.4%)	20 (43.5%)	5 (10.9%)	5 (10.9%)	1 (2.2%)
S11	9 (19.6%)	11 (23.9%)	14 (30.4%)	4 (8.7%)	6 (13%)	2 (4.3%)

The qualitative versus quantitative risk assessment is a well-known debate in ISRA [4], the former is mostly subjective knowledge-based and often describes risk using qualitative expressions, such as high, medium, and low. While the quantitative approach is mainly numerical and often based on statistical methods. There are arguments both for and against both approaches [4]. With the described issue at its core, we asked the participants to rank several statements regarding ISRAn practices, Table IX holds the statements with results and the distributions are in Table X. The results were diverse regarding all the statements, with the lowest median at 3 and highest at 5. In the following text, we analyze each statement with regards to descriptive statistics and correlation analysis. There are multiple differences between the three analyzed categories regarding nine of the statements, Table XI, and we analyze these differences together with the statement in question.

The results from Statement (S) 1, shows, with about 75% answering 4 or more, that most respondents consider their approach to be mainly qualitative. Worth noting is the minimum value of 2 in the results documenting that all of the participants consider their ISRAn methods to at least have some level subjectivity. S1 also has the highest median of 5 and lowest variability in the results. Regarding S2, less than half of the respondents consider their approaches to be more quantitative than qualitative, with 28% answering 5 or 6 indicating a mainly quantitative approach. Table XI shows that there is a notable difference between work types in this matter, whereas technical/hands-on practitioners view their approach as more quantitative. S2 regarding quantitative methods is also negatively correlated to S1 at the 0.05 level, Table XII.

In S3, regarding prediction of monetary costs, the median is 3 with a large variability in responses indicating that it is hard to predict the monetary cost of an incident based on ISRAn results. Also, the Expert group rated S3 lower than the other two groups, with the proficient group agreeing most with S3. Meaning that the experts in our sample find it harder to use the ISRAn results to predict the monetary cost of an incident.

The risks of being too reliant on expert predictions are that results can become too opinion-based, vulnerable to several external human factors, for example, emotional state and feelings [12], the Narrative Fallacy [13]), and involve a high degree of guesswork (see [4]). S4, regarding ISRAn reliance on expert predictions, the median is 4, with 87% of the responses being in the 3-5 range. There is notable difference between company sizes (Table XI), where small and medium companies seem more reliant on expert predictions than the enterprise-sized organizations.

Regarding S5, asks if spending resources on quantitative ISRAn are worth the results. The results show that majority (65%) answered 3 or less, while a minority (22%) answered 5 or more. However, there is a notable difference between technical and administrative work type (Table XI). Where the admin respondents consider quantitative risk assessments as a bigger waste of time than the tech respondents, which also corresponds to differences between these groups in S1 and S2.

Lack of historical data is claimed to be a consistent problem in InfoSec [4] and S6 addresses this issue. The median of 4 provides some evidence to support this assertion, there was also a notable difference between expert groups here, whereas the experts ranked this issue higher than the competent and proficient group.

Mathematical probability calculations is an issue with many opinions in the ISRA community [4], S7 and S8 connects to this issue. S7 addresses views on the adequacy of mathematical ISRAn methodology for probability calculations, with the results showing a difference of opinion on existing methods, the median of 3. There was a notable difference between the respondents from Small and Medium companies, ranking this issue higher than those from the Enterprises. The results are similar for S8, regarding Annual loss expectancy (ALE), although the difference is smaller for both total results and between the companies.

S9 addresses risk forecasting accuracy, and the results show that the respondents' general confidence in their predictions is on the low side. There was no notable difference between the expert groups indicating that confidence in precision has not improved with increased experience and expertise. However, there was a difference between company sizes, where the small and medium companies perceive a higher accuracy in their estimates. There is more complexity in larger organizations, which is one of the key challenges for prediction [14] and may be one of the causes.

Both S10 and S11 are connected to unforeseen incidents and causes, both related to Black Swan Risks [13] which are rare outlier risks that carry an extreme impact. Our results indicate that consequences of occurred incidents tend not be outliers and that causes for severe events/disasters are more often known than not. The analysis displays a difference between expert groups, with Experts being confident in their

knowledge about causes of incidents and disasters. From our results we see that most causes are believed to be known, and that Black and Grey Swan-type incident are very seldom. However, rare events and how they drive the InfoSec program is a path for future research.

This section has touched on one of the key challenges in ISRA, which is obtaining quantitative estimates of the probability of occurrence for security incidents, together with a reliable estimate of the consequence in a methodologically sound way. Which is difficult because of several reasons [14], [4], [10], where the factors that limit the forecasting are, for example, complexity, interconnectivity, and active adversaries. These factors do not apply for all InfoSec risks [14] and there is utility in obtaining statistical distributions of InfoSec risks [14]. As our results have shown, there are degrees of subjectivity to every risk assessment and one area to strengthen research is in risk quantification by working on obtaining probability distributions. In addition to combining both the quantitative and qualitative estimates in the risk model.

TABLE XI. NOTABLE DIFFERENCE BETWEEN CATEGORIES (FULL STATEMENTS CORRESPOND TO NUMBERS IN TABLE IX)

Statement	**Expertise**	N	Min	Max	Range	Median	Grouped Median
S3	Comp	9	2	5	3	3,00	3
	Proficient	17	1	6	5	4,00	3,80
	Expert	20	1	5	4	3,00	2,56
S6	Comp	9	2	5	3	4,00	4,17
	Proficient	17	1	6	5	4,00	3,70
	Expert	20	2	6	4	5,00	4,73
S11	Comp	9	1	5	4	4,00	3,75
	Proficient	17	1	6	5	3,00	2,70
	Expert	20	1	5	4	2,50	2,33
	Company Size						
S4	Enterpr	26	1	5	4	3,50	3,62
	Medium	8	3	5	2	4,50	4,33
	Small	12	3	6	3	4,50	4,38
S7	Enterpr	26	1	6	5	3,00	3,07
	Medium	8	2	6	4	5,00	4,60
	Small	12	2	6	4	5,00	4,71
S8	Enterpr	26	1	6	5	2,50	2,50
	Medium	8	2	6	4	2,50	2,67
	Small	12	1	6	5	3,50	3,67
S9	Enterpr	26	1	5	4	3,00	2,75
	Medium	8	2	6	4	3,00	3,25
	Small	12	3	6	3	4,00	3,88
	WorkType						
S1	Technical	17	2	6	4	4,00	4,27
	Admin	29	2	6	4	5,00	4,71
S2	Technical	17	1	6	5	4,00	4,00
	Admin	29	1	6	5	3,00	2,71
S5	Technical	17	1	5	4	3,00	2,73
	Admin	29	2	6	4	3,00	3,44

C. Correlations between statements

Several of the statements have strongly correlating results, Table XII. There is an interesting correlation regarding S2 on quantitative and statistical ISRAn methods: S2, is strongly correlated with S3 and S8, and weakly correlated with S9 and S11. The former correlations indicate that applying quantitative methods makes it easier to convert ISRAn results into monetary costs of incidents. The weak correlation to S9 indicates that working with risk quantification can improve precision and confidence in risk estimates. S3 is also strongly correlated with S8 and S9 further indicating that there are benefits from working with quantification and monetizing risk estimates. S3 is also negatively correlated with statement 1 in Table VII; *Assigning Monetary value to an information asset is difficult*. Further, the correlations test between the two sets of statements also indicates that gathering precise knowledge regarding asset value (36_5) correlates with confidence in consequence estimate precision. Another finding from this table is that prioritizing assets security as more important than stable operations (36_4) correlates with less insight into causes for severe incidents (S11).

Being reliant on expert predictions (S4) correlates strongly with the lack of historical data problem (S6) and lack of mathematical approach (S7) to ISRAn probability calculations. However, expert predictions also correlate with precision (S9), it seems a combination of mathematical models and expertise is then optimal. Lack of historical data (S6) also correlates with S10 and S11, indicating that historical data is necessary to prevent outliers and discover causes.

One Admin expert commented that *"Mathematical probability calculations are not worth anything if the organization does not believe in the probability of an incident occurring. Math alone is not the issue here. It is about the human ability to not just identify risk but accept risk presence (for real and react before the consequence of a corresponding issue hits)"*. Another Admin expert commented that *"There is still a lack of understanding of threat assessment as an input to identifying an actual risk."* The latter statement touches on the intersection between qualitative and quantitative methods since threat assessments are mainly subjective and can be more comprehensive than a purely quantitative approach being limited to observed data.

Consider the complexity and many aspects of loss calculations; one admin proficient commented: *"We consider the impact to business of loss of business (future) / customer impact, loss of reputation / brand impact, legal or regulatory breach and loss of money / financial impact."* Which highlights the many variables that must be considered in such calculations.

TABLE XII. CORRELATIONS BETWEEN ISRAN STATEMENTS. (FULL STATEMENTS CORRESPOND TO NUMBERS IN TABLE IX)

Statements		S2	S3	S5	S6	S7	S8	S9	S10	S11
S1	Pearson	-.367*		.333*	.363*					
	Sig.	,012		,024	,013					
	N	46		46	46					
S2	Pearson	1	.536**				.481**	.345*		.336*
	Sig.		,000				,001	,019		,022
	N	46	46				46	46		46
S3	Pearson		1				.440**	.425**		
	Sig.						,002	,003		
	N		46				46	46		
S4	Pearson				.443**	.385**		.400**	.474**	
	Sig.				,002	,008		,006	,001	
	N				46	46		46	46	
S6	Pearson				1	.414**			.460**	.321*
	Sig.					,004			,001	,030
	N				46	46			46	46
S8	Pearson						1	.428**		.337*
	Sig.							,003		,022
	N						46	46		46

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

D. Application of ISRAn methods and concepts

To obtain an insight into industry practice and adaptation of methods and concepts we compiled a non-exhaustive list of popular risk assessment tools and concepts, and asked how often they applied them in their ISRAn practice. Table XIII displays how the concepts were ranked by the participants. The three most frequently used methods are Business Impact Analysis, Penetration tests, and Security scanners, all with a median of 5. Cascading/correlating risks are the most

frequently applied concept for risk analysis. The items from *Component Testing* down to *Common Mode Failure* have medians between 3-2. The results show that methods for different genres of risk assessment (collected from [15], [13], [16]), such as Fault and Event tree analysis, HAZID, and HAZOP, are not common in ISRAn, where practitioners prefer methods developed specifically for InfoSec. Common concepts such as Black Swan Risks [13] and ALARP (As Low As Reasonably Practicable) [15] are also not widely known and applied by the surveyed practitioners. One admin expert commented on this particular issue: *Fault Tree Analysis, FMEA [Failure Mode and Effect Analysis], Hazop etc. are usually methods used by safety professionals, not information security professionals (I have however used them both but for slightly different purposes) and MTF or MTBF (Mean Time Before Failure) is typically also used in these safety oriented methods. I see the ability to merge methodologies between these areas of expertise for mutual benefit, but as far as I know, the industry does not do that in current operation.*

The same expert also commented on the three of the item's role of tools in reducing uncertainty: - *Different tools are in use for different purposes. I do not see penetration testing/security scanner/component testing as part of risk analysis. It is additional tools relevant to use if the risk evaluators are unable to be certain about probability - such testing can document probability and it also provides low-level insights to mitigation means.*

TABLE XIII. APPLICATION OF TOOLS, METHODS, AND CONCEPTS IN ISRA. (SCALE: 1 - UNFAMILIAR, 2 - VERY SELDOM, 3 - SELDOM, 4 - SOMETIMES, 5 - OFTEN, 6 - VERY OFTEN)

		N	Min	Max	Median	Range	Mean	Variance	Category
1	Business Impact Analysis	46	1	6	5	5	4,63	2.016	Method
2	PenTest	46	1	6	5	5	4,5	1,722	Method
3	Security Scanners	46	1	6	5	5	4,3	2,528	Concept
4	Cascading Risks	46	1	6	4	5	3,39	2.999	Method
5	Component Testing	46	1	6	2,5	5	2,96	3.109	Method
6	Mean Time To Failure	46	1	6	2,5	5	2,8	2,516	Method
7	Event Tree Analysis	46	1	6	2	5	2,93	2,773	Method
8	Fault Tree Analysis	46	1	6	2	5	2,65	2,810	Method
9	ALE/SLE	46	1	6	2	5	2,61	2.866	Method
10	FMEA	46	1	6	2	5	2,57	3.007	Method
11	Attack Trees	46	1	6	2	5	2,48	2,477	Method
12	OCTAVE	46	1	6	2	5	2,17	2,191	Method
13	Monte Carlo Simulations	46	1	6	2	5	2	1,467	Method
14	Common Mode Failure	46	1	6	1	5	2,39	2.955	Concept
15	Bayesian Networks	46	1	5	1	5	2,11	1.566	Method
16	Black Swan Risk	46	1	5	1	4	1,98	1,977	Concept
17	Antifragility	46	1	6	1	5	1,87	1.805	Concept
18	ALARP	46	1	6	1	5	1,7	1,416	Concept
19	CORAS	46	1	5	1	4	1,7	1.372	Method
20	HAZOP	46	1	5	1	4	1,65	1,032	Method
21	HAZID	46	1	5	1	4	1,61	1,088	Method

E. Cost-effectiveness of ISRA methods

As a follow up, we asked the participants which ISRAn method they considered to be most cost-effective, in which we received ten answers. There were no clear answer to this inquiry: Two Admin experts argued for Business Impact Analysis (BIA), as *"at the end of the day the systems that our business use are our main reason to have an IT area"*, and it *"can be done without bringing in external resources"*. BIA contains several tools and methods for reducing uncertainty related to consequences of risks.

Two argued (Admin expert and proficient) for security scanners and penetration tests (pentests), as *"they provide undeniable evidence of vulnerabilities. It is hard for someone to argue with them."* While two respondents (Admin expert and proficient) argued for the use of *Bowtie*-diagrams based on cause, threat, and risk analysis. We do not find Bowtie diagrams extensively described in the ISRA literature, although they are found in the more generic safety-related risk assessment literature, such as [15]. Bowtie are used for both risk analysis, visualization and communication.

F. What is the most important task of the ISRA?

There several tasks that are common when conducting an ISRAn [17], we gathered the common denominators and asked the participants to rate them according to their importance, 1 - Not important to 6 - Very important. Table XIV displays the results, with no notable difference between any groups. The participants ranked all the items highly, with lowest median being 4. The low end of the scale contains importance of knowledge about Stakeholders, Attacker capability, and Uncertainty. Whereas the remainder of the items are rated 5 or higher, meaning they are essential to the process. The respondents ranked Impact/consequences and threat as the most important tasks for the ISRA work.

TABLE XIV. VIEWS ON IMPORTANCE OF TASKS AND ITEMS FOR RISK ANALYSIS. (SCALE: 1 - NOT IMPORTANT, 6 - VERY IMPORTANT)

	N	Min	Max	Median	Range	Mean	Variance
1. Asset	46	1	6	5.5	5	5,15	1.287
2. Threat	46	3	6	6	3	5,33	0,936
3. Guardian/Control	46	3	6	5	3	5,02	1,133
4. Uncertainty	46	1	6	4	5	4,24	1,742
5. Probability/Likelihood	46	3	6	5	3	5,2	0,828
6. Impact/Consequences	46	3	6	6	3	5,37	0,638
7. Stakeholders	46	1	6	5	5	4,5	1,9
8. Attacker Capability	46	2	6	4	4	4,11	1,432
9. Vulnerability	46	3	6	5	3	5,24	0,586
10. Expert Knowledge	46	3	6	5	3	4,96	0,665

V. CHOOSING RISK TREATMENT STRATEGIES

Jaquith [18] claims that for most people, risk management really means risk identification, although these phases are clearly defined in the ISO/IEC vocabulary [1]. Applying ISO/IEC 27005:2011 [3] as a yard stick, the risk identification-phase clearly contains the majority of data collection and analysis. So, we asked the participants to rank the three different ISRA phases on importance. Table XV shows that the phases are almost equally ranked by our sample, with the risk identification scoring highest with a 6 median, otherwise, the difference between the phases are negligible.

TABLE XV. RANK THE PHASES OF THE ISRA PROCESS ACCORDING TO YOUR PERCEIVED IMPORTANCE, SCALE 1 (NOT IMPORTANT) - 6 (VERY HIGH IMPORTANCE)

	N	Min	Max	Median	Range	Mean	Variance
Risk Identification	46	4	6	6	2	5,57	,340
Risk Estimation	46	4	6	5	2	5,15	,532
Risk Evaluation	46	4	6	5	2	5,26	,464

Blakley et.al.[2] claims that the risk treatment strategies applied in IS focus primarily on risk mitigation, while transference, acceptance and avoidance as alternatives are seldom considered. The authors explain that the reason for this is the general approach to ISRM, where the practitioners are geared to imagining and then confirming technical vulnerabilities in information systems, so that steps can be taken to mitigate them. InfoSec activities rarely include any discussion of indemnity or liability transfer, although some organizations do address these issues in an "operational risk" organization

separate from the information security organization. Table XVI displays how the survey participants replied when we asked them how often they recommend the different risk treatment strategies for ISRA (scale 1 - Never, 2 - Very Seldom, 3 - Seldom, 4 - Sometimes, 5 - Often, and 6 - Very Often). Risk mitigation is the option ranked highest with 87% of respondents answering often or very often. This result supports Blakley et.al.'s claims about this strategy. However, the results also show that other strategies are frequently considered. The Blakley et.al. paper was written over a decade ago and the ISRA community may have matured in this area, although this is a field for future research. The *Transference* option is almost normally distributed, while the *Avoidance* option is bimodal with one top at *Sometimes* (39,1%) and one at *Very seldom* (19,6%). The *Acceptance/Retention* option is described by the median with 71% opting for *Sometimes* and *Often* alternatives. A clarification is provided by an admin expert with regards to type of industry: *"When it comes to health information, where regulatory requirements are very clear at placing the responsibility within the business, and a risk could lead to loss of life or health or patient confidentiality, transference is seldom an option."* Whereas another admin expert comment: *"Avoidance is seldom an option. Acceptance is most often already defined at some certain level in the business and is therefore most often not an option for any identified risks above defined threshold of acceptance. Optimisation is most often not prioritized until a result shows all risks identified to be below defined level of risk acceptance or as something to "think about" when all identified risks beyond acceptance threshold is reduced to a level within acceptable threshold."*

TABLE XVI. RESPONDENTS' RECOMMENDATION OF RISK TREATMENT OPTIONS IN ISRA. SCALE 1 (NEVER) TO 6 (VERY OFTEN)

	Valid	Min	Max	Median	Range	Mean	Variance
Transference	46	1	6	4,00	5	3,46	1,631
Mitigation	46	2	6	5,00	4	5,20	,872
Avoidance	46	1	6	4,00	5	3,76	1,608
Acceptance/Retention	46	2	6	4,00	4	4,15	1,065
Optimisation	46	2	6	4,00	4	4,30	1,150

Blakley et.al. also claims that InfoSec as a discipline focus more on reducing the probability of an event than on reducing its consequences. And where the focus is on reducing consequence, it tends to focus much more strongly on quick recovery (for example, by using aggressive auditing to identify the last known good state of the system) than on minimizing the magnitude of a loss through measures to prevent damage from spreading. We asked the participants which they thought more important, reducing the probability or consequence of the risk. Fig. 5 shows that the results are almost 50/50 distributed, no better than random. According our sample, there is no clear preference towards one or the other. With that said, this is often a two part process, where one can treat both probability and consequence of the risk to obtain a reasonable risk level. This issue was also highlighted to some extent by six of the twelve written comments to this question. The type of risk was also highlighted in four answers as a determining factor. One admin expert wrote: *"Proactive approach to risk reduction (i.e. probability) is most often chosen prior to reactive approaches (i.e. impact/consequence) as long as that is a feasible approach compared to cost of reactive approaches. The risk assessment result however, includes recommendations of both types for the business to conclude."* Also highlighting the need for cost/benefit analysis of the proposed risk treatment.

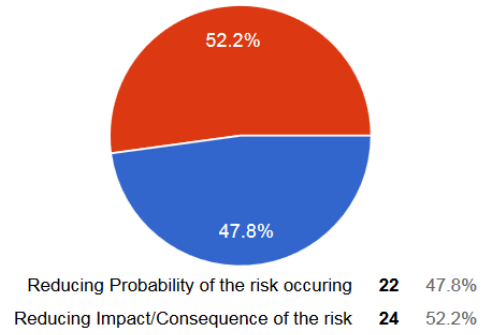

Fig. 5. Results from opting to reduce either probability or consequence

VI. SUMMARY & CONCLUSION

In this section, we first discuss the limitations of this study. Then, we conclude our findings, together with research implications and directions for future work.

A. Limitations

While our choice of online survey allowed us to recruit participants from our target group through specialized web-forums, this approach has some limitations. First of all, our data are self-reported values based on participants perceptions, while not a substitute for behavioral and observational data from real-world scenarios, this self-reported data can still provide valuable insight into day-to-day practices and how practitioners view the research problems. Furthermore, the study design and recruitment process gave us less control of the research participants; the control questions somewhat mitigated this problem, but these were not fool-proof, and circumvention was possible. The sample size was also small, although the online groups and forums exposed the survey to many potential respondents we only managed to recruit forty-six in one month. Based on the many members of these groups, the recruitment strategy was not a success. Many restricting factors could have caused this outcome, for example, activity in the forums, exposure of the survey, and questionnaire length. Although the sample had a good geographical spread and diverse background from the participants, this small sample is sensitive to outliers. The written responses and comments are more anecdotal evidence.

Another limitation of this study is concerning what is not asked for, issues we are not aware of or not present in the questionnaire can not be answered. We partially addressed this issue by adding with comment sections in the questionnaire, but this issue is likely better addressed in open interviews.

B. Conclusion & Future Work

InfoSec risk management and assessment are essential to well-functioning InfoSec program as it determines what to protect and how. In this paper, we have addressed three major areas of practice in ISRM and provided incentives to strengthen

research within them; on the ISRA level, we found that the majority did not differentiate between ISRA methods for different organizational tiers. However, several respondents did distinguish, for example through formality, and handled risks at the higher abstraction levels more formally. As a future direction, we propose to research handling and assessing risk between the organizational tiers, together with risk escalation issues.

Gathering the ISRA team and securing the right knowledge is essential to the assessment; Our results showed that the CISO/CSO and InfoSec personnel most frequently leads and attends risk assessments while various roles in IT department attends based on the scope of the assessment. Knowledge about information assets and business understanding was highlighted as essential, together with knowledge about laws & legislation stressing the importance of legal counsel in the ISRA. Composition and optimization of the ISRA team from the knowledge perspective is a potential path for future research.

Throughout the results, several respondents highlighted the significance of the risk assessors experience for the results, as *any method is only as good as the person executing it.* On qualitative and quantitative approaches, we found that the majority of ISRAn approaches are qualitative. While those who described their work as more technical were more likely to describe their ISRAn approach as quantitative. Our analysis shows that confidence in impact estimates precision tends to be low, however, working with risk quantification is likely to improve accuracy and trust in risk estimates. Which highlights the importance of both the expert and the benefits working with quantification. A path for future work is to research the intersection between these two approaches to optimize the ISRA results.

Related to the precision in impact estimation, we found that Black Swan theory is very seldom applied in ISRA. Possible paths for future work is an analysis of InfoSec risks and how they relate to Black Swans, together with research on rare events and how they drive the InfoSec program. We have provided incentives for strengthening research within obtaining probability distributions for frequencies and consequences for InfoSec, as this is an area that has a potential for producing useful knowledge for decision-makers.

Worth noting is that experts ranked the importance of threat intelligence for ISRA lower than the less experienced groups. On the risk analysis practices, this study documented that asset evaluation is a challenge, with experts considering the existing risk assessment methods as not sufficient to handle this problem. The participants also ranked knowledge about assets as important in multiple instances in the results which make asset evaluation stand out as an issue for future research.

From our list of suggested tools and concepts Business impact analysis, penetration tests, and security scanners are the most frequently applied tools for ISRA. Together with Bowtie-diagrams, these methods and tools are deemed the most cost-effective.

ACKNOWLEDGMENT

The Author thanks professors Einar Snekkenes for discussion, and my colleagues Andrii Shalaginov, Ambika Shrestha Chitrakar, Yi-Ching Lao and Goitom Weldehawaryat for quality assurance. Professor Stewart Kowalski for his knowledge on Likert-scales and analysis. We extend a thanks to all who answered the questionnaire, the anonymous reviewers for their comments, and the support from the COINS Research School for InfoSec.

REFERENCES

[1] *Information technology, Security techniques, ISMS, Overview and vocabulary*, International Organization for Standardization Norm, ISO/IEC 27000:2014. [Online]. Available: http://dx.doi.org/10.3403/30236519

[2] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001, pp. 97–104.

[3] *Information technology, Security techniques, Information Security Risk Management*, International Organization for Standardization Std., ISO/IEC 27005:2011.

[4] G. Wangen and E. Snekkenes, "A taxonomy of challenges in information security risk management," in *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger*, vol. 2013. Akademika forlag, 2013.

[5] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Information Management & Computer Security*, vol. 22, no. 5, pp. 410–430, 2014.

[6] G. Wangen, "An initial insight into infosec risk management practices," in *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2015 - Aalesund*, vol. 2015. Open Journal Systems, 2015.

[7] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management*, vol. 41, no. 5, pp. 597–607, 2004. [Online]. Available: http://dx.doi.org/10.1016/j.im.2003.08.001

[8] G. A. Churchill Jr, "A paradigm for developing better measures of marketing constructs," *Journal of marketing research*, pp. 64–73, 1979.

[9] G. Locke and P. Gallagher, "800-39 nist sp, managing information security risks - organization, mission, and information systems view," National Institute of Standards and Technology: U.S. Department of Commerce, Tech. Rep., 2008.

[10] S. Fenz and A. Ekelhart, "Verification, validation, and evaluation in information security risk management," *Security Privacy, IEEE*, vol. 9, no. 2, pp. 58–65, 2011.

[11] Y. Zhiwei and J. Zhongyuan, "A survey on the evolution of risk evaluation for information systems security," *Energy Procedia*, vol. 17, pp. 1288–1294, 2012.

[12] G. F. Loewenstein, E. U. Weber, C. K. Hsee, and N. Welch, "Risk as feelings." *Psychological bulletin*, vol. 127, no. 2, p. 267, 2001.

[13] N. N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. Random House LLC, 2010.

[14] G. Wangen and A. Shalaginov, *Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers*. Cham: Springer International Publishing, 2016, ch. Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security, pp. 127–143. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-31811-0_8

[15] T. Aven, W. Røed, and H. S. Wiencke, *Risikoanalyse (Norwegian Ed)*. Prinsipper og metoder, med anvendelser. Oslo: Universitetsforlaget, 2008.

[16] N. N. Taleb, *Antifragile: things that gain from disorder*. Random House LLC, 2012.

[17] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method compcomplete - core unified risk framework," in *[Under Revision]*. .., 2016.

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