An Initial Insight Into InfoSec Risk Management Practices

Gaute Wangen
Center for Cyber and Information Security,
NISlab, Høgskolen i Gjøvik
Gaute.Wangen2@hig.no

Abstract

Much of the debate surrounding risk management in information security (InfoSec) has been at the academic level, and how practitioners view predominant issues is an important element often left unexplored. Thus, this article represents an initial insight into the InfoSec risk professionals view of the field through the results of a 46-participant online study. We analyze known issues regarding InfoSec risk management (ISRM), especially concerning risk management program development and maintenance, contributions to business, and challenges within the research field. One of the key findings from this study was that risk communication is a key skill that likely needs more emphasis in InfoSec training. Also, we document several issues concerning security measurements and return on investment for the ISRM program, together with other relevant paths for future research.

1 Introduction

This paper investigates the practitioners view of research problems within information security (InfoSec) risk management (ISRM). While there is plenty of available material regarding what ISRM frameworks contain and how they compare with each other [7], the literature is scarce regarding the current ISRM industry practices. There are several known theoretical problems in ISRM[7], 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 an online survey and represents a step towards a more holistic picture of ISRM practices.

The main benefit of this paper is new knowledge regarding current practices in ISRM with emphasis on the risk management part. This study also provides new knowledge regarding where the research in ISRM should be focusing the efforts, making the ISRM community and researchers the main beneficiaries of this study. Improving ISRM is essential in making progress in the InfoSec research field as it is this process that helps determine organizations determine what and how to protect. Thus, the intended audience of this paper is InfoSec professionals and academics, together with other ISRM practitioners and stakeholders.

The main research question investigated in this paper is ”How does the risk management

This paper was presented at the NIK-2015 conference; see http://www.nik.no/.

problems outlined in previous work [7] reflect problems experienced in the industry?". Due to the width of the field, we have narrowed the scope of this research to investigate industry practices within Risk management, with the following scope:

1. How do industry practitioners view known issues regarding ISRM definitions, perceptions, development, and maintenance?
2. What do industry practitioners perceive as the biggest contributions of ISRM to the business?
3. What do industry practitioners consider to be the biggest challenges within ISRM?

The main goal of InfoSec is according to ISO/IEC 27000:2009 to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity, availability, and non-repudiation. Best practice InfoSec is highly dependent on well-functioning ISRM processes[2]. While ISRM is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve acceptance[1]. The issues investigated in this paper primarily builds on the findings of the survey paper "A Taxonomy of Challenges in ISRM" [7], whose main purpose was to categorize and present known research problems at different stages in the ISRM areas and activities.

The remainder of this article has the following structure. First, we describe the research method in the form of data collection approach and analysis. Following this is a discussion of the results in terms of the research questions and implications, including limitations of this study, and lastly we conclude the paper.

2 Research Method

This study was conducted to investigate ISRM industry practices and the respondents' views of several known challenges within the research field. 46 participants completed our online survey which asked about issues from the previously described taxonomy [7]. The first sub-section addresses the choice of data collection method and design to address the research questions. The second sub-section presents a brief overview of the statistical methods used for data analysis.

Data Collection - Online Questionnaire

One of the most prominent problems in InfoSec studies is getting in touch with the target group and acquiring respondents [4]. One potential explanation for this is that InfoSec research is one of the most intrusive types of organizational research. Also, that there is a general mistrust of any "outsider" attempting to gain data about the actions of the security practitioner community [4]. Thus, non-intrusiveness is an important requirement when designing the data collection tool. The narrow target group, industry professionals, made obtaining respondents a challenge as the study was subject

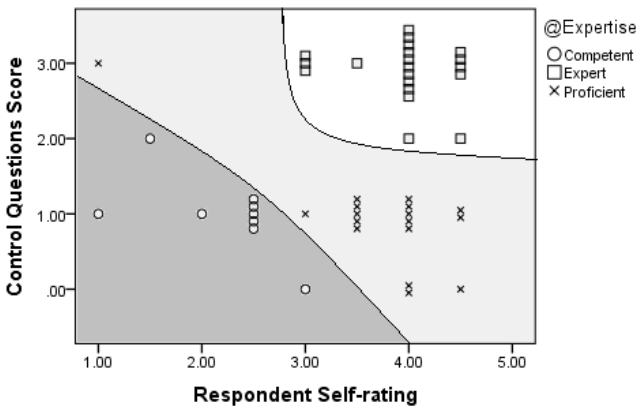

Figure 1: How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)

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 no control of participants except that they are members of particular forums, Table 1. 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 [3]. As for the level of measurement, the questionnaire had category, ordinal, and continuous type questions. Category type questions mainly for demographics, while the main bulk of questions were designed using several mandatory scale- and ranking questions. 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 primarily risk management.

Table 1: 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

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 applied in this research is as follows [5]:
For *Descriptive analysis* we have considered distributions including range and standard deviation. On continuous type questions, we applied measures of central tendency (average) mean, median and mode. We also conducted *Univariate* analysis of individual questions, and *Bivariate* analysis for pairs of questions, such as a category and a continuous question, to see how they compare and interact (means and standard deviations). *Crosstabulation* was applied to analyze the association between two category type questions, such as ”Company Size” and ”Expertise”. We applied *Scatterplot* to visualize two or more continuous type questions.
We have applied *Inferential Statistics* as a basis for making predictions and determining significance. The analysis has primarily operated with a standard 95% confidence interval (CI), but we have also included results withing a 90% and 85% significance, applying ANOVA for tests of statistical significance. We applied the Turkey post hoc tests to analyze further statistically significant results between pairs and reveal relationships between variables. We have applied Pearson *Correlation test* to reveal relationships between pairs of continuous type variables.

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.

3 Results

This section contains the results of the statistical analysis, starting with demographic data. Further, we present the results from investigating each research question; firstly, the data analysis of risk definitions and ISRM perceptions, scope and development. Following this with the analysis of the main contributions and challenges of the ISRM program.

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

Respondents and Demography

The questionnaire was deployed on specialized InfoSec risk forums on LinkedIN.com, Table 1, where we received 46 accepted answers. See Table 2 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.

Risk Definitions

We find one of the issues with the ISRM vocabulary in the many definitions of what an InfoSec risk is [7]. So, we provided the participants with a set of risk definitions from various standards, methods, and literature, and asked which definition they thought best described an InfoSec risks, Table 3. This issue is important in determining the philosophical approach to risk, for example if the probability is central to risk or not. One of the Experts reported that he agreed with the ISO/IEC

Table 2: Classification of Respondents, total 46.

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

27005:2005 definition, and added: *"... Replace "the organization" with "individuals"."* Whereas another Expert commented: *"My definition of the Risk Management Process would include this: "that influences how well they achieve their objectives".*

ISRM perceptions, scope, and development

Responsibility for the ISRM program is important in the context of determining whether InfoSec is perceived as mostly a technical discipline and an IT issue and importance to

Table 3: Results from asking ”Which definition best describes an InfoSec Risk in your opinion?”

Definition	**N**	**%**	**Source**
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.	31	67.4%	ISO/IEC 27005:2005
The Effect of Uncertainty on Objectives	4	8.7%	ISO/IEC 31000:2009
Threat * Vulnerability * Asset	4	8.7%	Computer and Information Security Handbook (2009)
((Vulnerability * Threat) / Counter Measure) * Asset Value at Risk	4	8.7%	`www.IT-Risk-Management.com`
Exposure to the chance of injury or loss; a hazard or dangerous chance	0	0 %	Dictionary.com Definition
Other	3	6.5%	

business. We asked the participants who was responsible for the ISRM program in their organization; the results showed that 54.35% has a CISO/CSO in charge of the program, and 15.22% of respondents has either the CEO or the Head of IT department in charge. None of the Experts reported the head of the IT department as responsible for the ISRM program. However, when we asked them to rate if the ISRM program was mostly run by the IT department about 50% agreed (answered 4-6) to this Statement, Table 4.

Table 4: Answers to ”Our ISRM program is ran by our IT department” sorted by company size.

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Min	Max	ANOVA
					Lower Bound	Upper Bound			
Small	12	2,58	1,832	,529	1,42	3,75	1	6	
Medium	8	3,25	1,488	,526	2,01	4,49	1	5	
Enterpr	26	3,81	1,767	,346	3,09	4,52	1	6	
Total	46	3,39	1,782	,263	2,86	3,92	1	6	0.14

We asked the participants how important they considered the ISRM process to be in achieving InfoSec, on a scale 1 (Unimportant) to 10 (Crucial). The results showed a mean value = 8.6 and Std.Dev. = 1.3. We also asked if the participants thought the cost of developing and implementing the ISRM program superseded the benefits the respondents were more divided, mean = 5, Std.Dev.= 2.7, with no significant difference between groups. This question prompted several comments from the respondents. Notably, three respondents commented on the difficulties of measuring benefits from an ISRM program and recommended *cost/benefits analysis* to make the business case for ISRM. Another administrative expert commented: *”Any risk management process in use has to be tailored to the business using it for it to be any sorts of the beneficiary at all. Tailored and actively in use it will be efficient and beneficiary.”* In addition, two experts commented on the importance and difficulties of keeping ”the big risk picture”, and to *”cope with the large amount of security measures that comes out of all the ”stand-alone” risk assessments that are performed.”*

The respondents were asked to rank several statements regarding the development and properties of their ISRM program on a scale from ”1 - Strongly Disagree” to ”6 - Strongly Agree”, Table 6. All the participants to various degrees based their choice of ISRM approach on recommendations from Experts or others, showing no significant difference in responses between company sizes or expertise. The respondents were asked if they mainly developed their ISRM approach themselves. Only 11% of the respondents agreed entirely with this statement, with a mean = 3.65 it is evident that most of the respondents’ companies do not primarily develop their own approach to ISRM. Further, we asked if

the respondents ISRM program was based on industry standards, none of the respondents strongly disagreed to this statement. There were differences between the expertise groups in this area, Table 5 , the results were statistically significant within 90%, and the Post-Hoc Turkey test showing significance between the Expert and Competent groups at P=5,5%. Showing that the Expert group is more likely to apply industry standards for their ISRM development.

Table 5: Differences in application of industry standards for ISRM program development

	N	Mean	Std. Deviation	Std. Error	95% CI for Mean Lower Bound	95% CI for Mean Upper Bound	Min	Max	ANOVA sig.
Competent	9	4,00	1,323	,441	2,98	5,02	2	6	
Proficient	17	4,71	1,263	,306	4,06	5,36	2	6	
Expert	20	5,15	1,089	,244	4,64	5,66	3	6	
Total	46	4,76	1,251	,184	4,39	5,13	2	6	0.068

The ISRM literature lists several claims regarding the scope of ISRM being too technical [7]. In support of these claims, we found that 58.6% of the respondents consider their ISRM program to include mostly technical solutions and ICT. However, 85% of the respondents reportedly consider Human factor risks as a part of their assessments.
Several actors have previously highlighted the need for data sharing within the InfoSec domain [7]. We found from our study about 75% of the respondents reports to be reluctant to share data about their ISRM program with other market actors, while 26% of these 75% never share data.
We found several correlations in the ratings, for example periodically measuring the performance of the ISRM program strongly correlates with working on improvements to the program (Pearson = 0.94), Table 6.

Table 6: Means, Std.Dev & Pearson Correlations between statements on a scale between 1 (Strongly disagree) - 6 (Strongly Agree). X-axis numbers corresponds to numbers on Y-axis.

Means and Correlations

				27_1	27_3	27_4	27_5	27_6	27_7	27_8
27_1 We chose our ISRM approach based on recommendation from Experts or others	Mean	3,91	Pearson Correlation	1						
	Std.Dev	1,244	N	46						
27_3 Our ISRM Approach is part of a larger ERM program	Mean	3,67	Pearson Correlation		1					
	Std.Dev	1,77	N		46					
27_4 Our ISRM program is based on industry standards	Mean	4,76	Pearson Correlation		0,424**	1				
	Std.Dev	1,251	Sig. (2-tailed)		0,003					
			N		46	46				
27_5 We periodically measure the performance of our ISRM program	Mean	4,09	Pearson Correlation		0,587**	0,671**	1			
	Std.Dev	1,561	Sig. (2-tailed)		0	0				
			N		46	46	46			
27_6 We work to improve our ISRM based on the results from periodic measurements	Mean	4,11	Pearson Correlation		0,596**	0,655**	0,94	1		
	Std.Dev	1,524	Sig. (2-tailed)		0	0	0			
			N		46	46	46	46		
27_7 We share data about our ISRM program with other market actors	Mean	2,52	Pearson Correlation		0,393**		0,313*	0,347*	1	
	Std.Dev	1,362	Sig. (2-tailed)		0,007		0,034	0,018		
			N		46		46	46	46	
27_8 We periodically measure the efficiency of our security controls	Mean	4,35	Pearson Correlation	0,334*	0,386**	0,693**	0,717**	0,719**	0,334*	1
	Std.Dev	1,303	Sig. (2-tailed)	0,023	0,008	0	0	0	0,023	
			N	46	46	46	46	46	46	46
27_11 Managing the human factor is not a part of our ISRM program	Mean	2,35	Pearson Correlation			-0,403**				
	Std.Dev	1,464	Sig. (2-tailed)			0,006				
			N			46				

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

Choice of industry standard

We got twelve comments on the rating questions, especially regarding the choice of industry standards. Seven mentioned the ISO/IEC 27000-series as their preferred approach to ISRM, one respondent reasoned this with ISO/IEC being *"well developed and mature standard"*. Four preferred the NIST-standards, but three of these mentions was as a supplement to the ISO/IEC standards. Two mentions of COBIT as either supplement or compliance audits. Others mentioned industry codes of conduct, ISF (IRAMM), OCTAVE Allegro, DIACAP, and RMF, as their preferred approaches.

Comments on measuring efficiency of the program.

Measuring security is one of the key problems in the InfoSec community [7] and several of the respondents commented on this issue. One approach described by a tech expert: "We have a set of IA controls [Information Assurance] and security technical implementation guides, each has a test or tests. A scorecard is used to document and evaluate compliance. Additionally various scanning tools are used. The results of these are put into a risk assessment report to summarize the risk to the system being evaluated."
Another approach described by a respondent from the same group: "Our measurement is based on the number of incidents as well as a number of deviations from the defined process. Lesser incidents and lesser deviation from the established process means we are achieving the results. Also, a non-availability of data via VPN for more than 30 min is also considered as an incident. The user has to inform the team if a connection fails to establish for more than 15min Redundancy has been built using multiple channels."
One administrative expert suggest audit findings, InfoSec events response, and contingency together with threat intelligence as security measurements and inputs to the risk assessment. Also, another administrative expert added "We measure how many systems have the approval to operate, the percent of systems patched, anti-virus, system weaknesses identified through assessments, and system log files." Other experts mentioned penetration tests and total service efficiency/quality as approaches to measuring security. The proficient respondents also reports to apply asset availability, asset reliability, and a number of incidents as measures of security. Another proficient mention subjective measures of control effectiveness.

Table 7: Perceived contributions of the ISRM program to different areas

	N	Minimum	Maximum	Mean	Std. Deviation
29_1 Asset protection	46	2	6	4,78	1,172
29_2 Compliance with laws and regulations	46	2	6	4,87	1,166
29_3 Improved Corporate competitiveness	46	1	6	3,61	1,483
29_4 Increase Customer base	46	1	6	3,15	1,549
29_5 Increased Production	46	1	6	3,39	1,390
29_6 Managing Security Investments	46	1	6	4,04	1,366
29_7 Mapping ICT Business Criticality	46	2	6	4,37	1,199
29_8 Reliable and Secure Operations	46	2	6	5,02	1,043
29_9 Safeguarding Systems	46	2	6	5,02	1,064
29_10 Safeguarding Employees	46	1	6	4,11	1,479
29_11 Security Management	46	2	6	4,83	1,161
29_12 Threat Intelligence	46	2	6	4,28	1,344
Valid N (listwise)	46				

Contributions of the ISRM Program

Applying the scale 1-6, where 1- Not Significant, 6- Very Significant, we asked the respondents "How would you rate the contributions of your ISRM program in the

following areas of your organization", see Table 7 for the descriptive results. Statistically significant findings are listed in Table 8. We found a significant difference in the views of ISRM contribution to *Increasing Customer Base* with regards to company size. The bigger companies viewed ISRM as more important in increasing the customer base; this relationship was also found in the correlation analysis with a Pearson = -0.416. Another significant finding (within 90% confidence) was regarding the *Increased Production* statement, the difference in views between the respondents from the smaller companies and the enterprises. The participants from the smaller and medium companies thought ISRM to be contributing more to production. Another thing to note is that no one from the Enterprise-sized companies answered 6 on either questions (29_4 & _5).
Another difference in views from company size was regarding *Mapping ICT Business Criticality*, whereas respondents from Enterprises perceive ISRM to have least effect, inverse Pearson correlation = -0.389. There was also difference in perceptions from the different expert groups (not significant), both Proficient and Expert respondents had a mean of 4.5 while the competent group had 3.9. The views on *Managing Security Investments* differed between work types, where the respondents with technical tasks thought of the ISRM program as more important than those with administrative tasks.

Table 8: Statistically significant findings from ISRM contributions

Area and ANOVA	Class	N	Mean	Std. Dev.	Std. Error	95% CI for Mean		Min	Max	Post Hoc Turkey Test
						Lower Bound	Upper Bound			
29_4 Increase	Small	12	4,00	1,758	,508	2,88	5,12	1	6	Sig.=0.018 Small-Entrp
Customer Base,	Medium	8	3,75	1,389	,491	2,59	4,91	2	6	Sig.=0.117 Med-Enterp
Sig=0.012	Enterpr	26	2,58	1,270	,249	2,06	3,09	1	5	
	Total	46	3,15	1,549	,228	2,69	3,61	1	6	
29_5 Increase	Small	12	3,92	1,621	,468	2,89	4,95	1	6	Sig.=0.136 Small-Enterp
production,	Medium	8	3,88	1,356	,479	2,74	5,01	2	6	
Sig=0.091	Enterpr	26	3,00	1,200	,235	2,52	3,48	1	5	
	Total	46	3,39	1,390	,205	2,98	3,80	1	6	
29_7 Mapping ICT	Small	12	5,00	1,348	,389	4,14	5,86	2	6	Sig.=0.03 Small-Enterp
Business Criticality,	Medium	8	4,75	,886	,313	4,01	5,49	3	6	Sig.=0.205 Med-Enterp
Sig=0.024	Enterpr	26	3,96	1,076	,211	3,53	4,40	2	6	
	Total	46	4,37	1,199	,177	4,01	4,73	2	6	
29_6 Managing	Tech Work	17	4,59	1,121	,272	4,01	5,16	2	6	
Sec Investments,	Admin Work	29	3,72	1,412	,262	3,19	4,26	1	6	
Sig=0.024	Total	46	4,04	1,366	,201	3,64	4,45	1	6	

Purpose behind doing ISRM work

We asked the participants what they thought were the main purpose behind doing ISRM work. Twenty-seven participants answered this voluntary written question. Several respondents listed multiple reasons for doing ISRM; we categorized the answers into four primary purposes: (i) Fifteen of the respondents answered *compliance* and requirements from laws and regulations as the primary reason for doing ISRM work. (ii) Nine respondents listed *protection* of the confidentiality, integrity and availability of assets, personnel, data, etc., as a primary reason for conducting ISRM. (iii) Nine listed *governance and risk management* purposes, such as aligning security efforts to business strategy and goals, balancing investments, and improving decision-making. (iv) Eight listed maintenance of *trust and reputation* in terms of internally, partners, and competitiveness as a primary reason.

Challenges in ISRM practices

We asked the participants what they considered the biggest challenges within ISRM. Twenty-five respondents answered this voluntary written question. Eleven respondents

mentioned aspects of risk communication issues as a core issue: One predominant issue was securing the buy-in of management and other stakeholders and securing continuous funding. This together with difficulties in making the return on investment and benefits from ISRM visible and lack of understanding of InfoSec risk from management, make up the main points from answering this question.
In addition, issues with aligning InfoSec efforts with business strategy and goals. For example, preventing the InfoSec controls from becoming an extra overhead onto normal operations instead of an inherent part of it, were mentioned as important challenges. Another highlighted issue was adapting to and dealing with the security issues from new technology and data mobility. One respondent highlighted human risks as the biggest challenge: *"Human behavior in this order of priority: 1. Executive non-accountability 2. Untrained business staff 3. Negligent IT staff 4. Unaccountable middle management 5. External activity.*

4 Discussion

In this section, we discuss our findings with respect to the research questions and their implications. Starting with risk definitions, responsibilities, development, and security measurements. Further, this sections discusses our results in terms of main contributions of and challenges for the ISRM. Lastly, we discuss the limitations of this study.
Our results show that there is broad agreement on what an InfoSec risk is (Table 3). The preferred ISO/IEC 27005:2005 risk definition is built on the classic *Risk = Probability x Consequence* and provides a foundation for a common understanding of InfoSec risk. This finding is in contrast to InfoSec risk assessment methodologies that have removed probability from the assessments, such as the OCTAVE approaches and the new Norwegian Standard 5831:2014. No other scientific disciplines that we are currently aware of defines risk without probability. Obtaining statistical probability distributions for InfoSec risks are inherently difficult due to the complexity of the field [6], but qualitative probability estimates are a viable approach where such data is lacking. This approach is likely the superior approach compared to avoiding probabilities entirely.
It is clear that the professionals view ISRM as crucial to achieving InfoSec in an organization. There were conflicting views on if the cost of developing and implementing the ISRM was worth the results, which indicates that developing a formal ISRM program creates a lot of overhead. A future path to pursue regarding this is if practitioners consider ad-hoc risk assessments to be superior to formalized approaches.
Our results indicate that practitioners view InfoSec as more than a technical discipline (Table 6). We also observed this in the results showing that 70% of the respondents' organizations had either CISO/CEO or similar roles in charge of the program. The CISO is ideally placed high in the corporate hierarchy to ensure broad influence to make InfoSec an organizational responsibility. Concerning responsibility, we also found that bigger companies are more likely to have the IT department run the ISRM program. One possible cause for this is that it is easier to include people in smaller companies, as these are generally more adaptable. Besides, 85% of the respondents reports to include human factor risks in their assessments, which shows that InfoSec risk assessments are assuming a more holistic scope than previously assumed [2]. 58.6% reports their programs to mainly include technical solutions and ICT, which in itself seems sensible since a large percentage of InfoSec is technical. We, therefore, do not consider these results as conflicting, but rather parts of a larger picture. Table 6 also shows a significant correlation (-0.403) between basing the ISRM program on industry standards and managing the

human factor.
There are many InfoSec standards and approaches to choose from and limited data on which standards are superior to others [7]. Over half of the respondents reports recommendations from others as deciding factors when it comes to choosing ISRM approach. One respondent commented that local legislation determines that they have to apply industry standards/codes of conduct specially developed for the industry. This aspect has potential for further research, for example if these specialized standards outperform the more generic approaches.
Our inquiry showed the ISO/IEC 27000-series as popular approaches to ISRM. We also found that some of the practitioners preferred to use the 27000-series in combination with other approaches, E.G. NIST, suggesting that there is room for improvement in the standards. One respondent commented on the need for the supplication of material for dealing with privacy issues. Choice of ISRM approach is one area that needs more research, in terms of determining if the differences between them matter for the security levels of the organization. The differences between expertise groups also showed that the experts were more likely to rely on industry standards, which is interesting, as we would expect the situation to be the reverse, perhaps indicating overconfidence in the less seasoned professionals?
Enterprise risk management (ERM) is a trend where one gathers all risk management programs into one program. According to the results, this trend has a medium penetration in the InfoSec community. However, the ISRM program being a part of a larger ERM correlates significantly with views on measurements, improvements, and data sharing. One respondent provided an insightful comment on InfoSec in project management: *"We track all levels of corporate projects to verify we have completed a risk assessment during the design phase of the project."* This is the spirit of "an ounce of prevention is worth a pound of cure", which has proven repeatedly to be a sensible risk management strategy.
Measuring security is one of the most challenging and vital aspects for improving InfoSec. We found a significant correlation between basing the program on industry standards and measuring the performance of the ISRM program (Table 6). There is likely a cause and effect relationship between these two variables where the emphasis on measurements in standards guides the InfoSec work. The results from questions regarding periodically measurements and working with improvement have similar means and are significantly correlated. The means were relatively high, 4.09-4.35, indicating that the InfoSec community prioritizes measuring security. The respondents suggested several metrics, however, one expert respondent had an insightful answer that ensures accountability: *"Measure is - That the management team is actively managing the top 3 risks."*

On the contributions of the ISRM program to business, the results show that the contribution is largest in safeguarding systems and ensuring reliable and secure operations (Tables 7 & 8). With compliance, security management, and asset protection viewed as the second biggest contributions. More interesting are the low scores on the business-related areas, improved corporate competitiveness, increased customer base and increased production. One respondent commented *"Increase Customer Base = keep public trust"*, but this perception does not seem to be shared by the majority of our respondents. The results show significant differences between company sizes, where the respondents from smaller companies perceive the ISRM program to be contributing more to business related areas. There can be several reasons for this; for example the size and complexity of enterprises make the effect of controls less visible. Or employees in larger companies may view the risk treatments suggested by the ISRM program as a hindrance in daily

operations. While it is easier to communicate the need for and effect of security controls in smaller companies. Another aspect is the certification regime; where a company needs certification to qualify for contracts (E.G. PCI-DSS in payment card industry). It is reasonable to believe that the ISRM program contributes to increasing the customer base in these cases, but the certifications may not be so popular as to influence visibly the results in this paper.

We also documented compliance with laws and regulations as the primary driver behind ISRM. Compliance requirements are useful in establishing a security baseline, but a risk-based approach should go beyond this and be tailored to manage overall organizational and operational risks. The risk management aspect was also reflected in our findings as both asset protection and general risk management/governance were listed secondary drivers. Maintaining trust and reputation was listed by eight respondents and emphasizes the public and financial impact a large-scale InfoSec incident can have for a company, and have become two key assets to safeguard. The main challenges listed by the respondents concerned risk communication issues, where securing management buy-in and funding for InfoSec projects were key. Risk matrices have been the target of most of the criticism of risk communication [7]. However, our results go beyond this, and implicate that communication and rhetorical skills are something that should have a larger emphasis on InfoSec training.

Not having a risk occur is a desirable outcome from a risk management process, but how does one visualize the return on investment in such a case? Several respondents highlighted this problem, and there is no easy answer to this. Keeping track of incidents and costs (E.G. annual losses) are popular measurements of InfoSec risk and visualizing effect. One respondent suggested measurements of service availability as an approach to visualize ISRM contributions, which is connected to the previously discussed problem of measuring security and is an area that require more research.

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 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. This outcome could have been caused by many restricting factors, 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 also sensitive to outliers.

5 Conclusion

This work has provided an initial insight into InfoSec risk practitioners view of ISRM. We conclude that the most popular risk definition is the ISO/IEC 27005:2005 version, which is based on the $R=PxC$ notion. Practitioners also view the ISRM process as

very important, but there were mixed views on whether developing a formal ISRM program was worth the cost. According to the risk professional, InfoSec is largely accepted as an organizational responsibility and not just a technical discipline. Although a large percentage of the respondents' organizations have managerial positions in charge of the ISRM program, Company size is one of the determining factors for where the responsibility for program implementation lie, as larger companies tend to have it ran by the IT department. The ISO/IEC 27000-series are popular ISRM approaches, but often in combination with other methods, suggesting that there is room for improvement in the standard. In terms of program maintenance, we found that measuring security is one of the most challenging aspects of InfoSec. Where basing the ISRM program on industry standards correlates positively with systematically working with measurements and improvements. The biggest contribution of ISRM to business is with safeguarding systems and ensuring reliable and secure operations. Respondents from bigger companies did not think the ISRM program to be contributing much to business-related areas, such as productivity. Compliance with laws and regulations was identified as the primary driver for doing ISRM work. From the practitioners point of view, the main challenges in ISRM are various aspects of risk communications. Especially, ensuring buy-in and continuous funding for InfoSec projects, and visualizing the benefits from the ISRM program, which highlights the need for risk communication and rhetoric skill training in future InfoSec training.

Acknowledgments

We thank prof Einar Snekkenes, Andrii Shalaginov, Ambika Shrestha Chitrakar, Yi-Ching Lao and Goitom Weldehawaryat. We also extend a thanks to all who answered the questionnaire and to the anonymous reviewers for their comments. The PHD-student Gaute Wangen is sponsored by COINS Research School for InfoSec.

References

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

[2] 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.

[3] Gilbert A Churchill Jr. A paradigm for developing better measures of marketing constructs. *Journal of marketing research*, pages 64–73, 1979.

[4] Andrew G Kotulic and Jan Guynes Clark. Why there aren't more information security research studies. *Information & Management*, 41(5):597–607, 2004.

[5] Eric Vittinghoff, David V Glidden, Stephen C Shiboski, and Charles E McCulloch. *Regression methods in biostatistics: linear, logistic, survival, and repeated measures models*. Springer Science & Business Media, 2011.

[6] Gaute Wangen and Andrii Shalaginov. Quantitative risk, statistical methods and the four quadrants for information security. In *Proceedings of the Tenth International Conference on Risks and Security of Internet and Systems, 2015. CRiSIS'15*, Lecture Notes on Computer Science. SpringerLink, 2015.

[7] Gaute Wangen and Einar Snekkenes. A taxonomy of challenges in information security risk management. In *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger*, volume 2013. Akademika forlag, 2013.