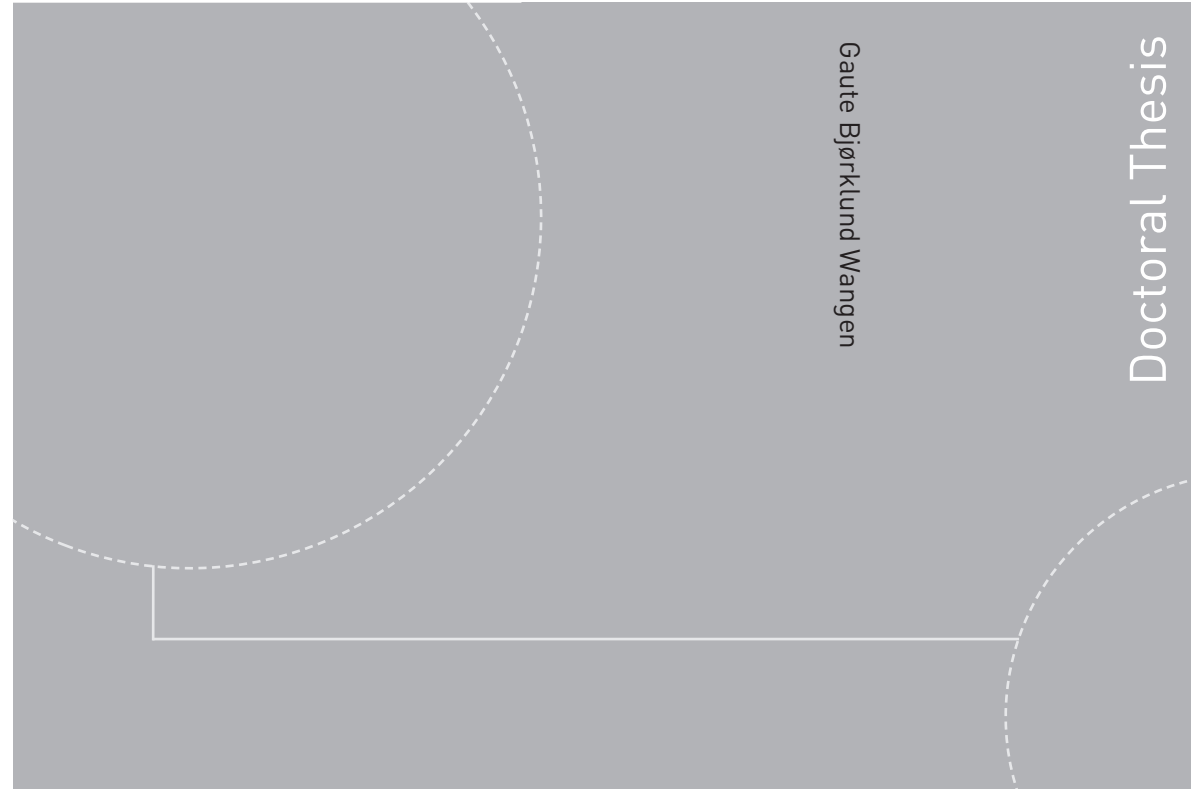


ISBN 978-82-326-2378-5 (printed version)
ISBN 978-82-326-2379-2 (electronic version)
ISSN 1503-8181



Doctoral theses at NTNU, 2017:153

Gaute Bjørklund Wangen
**Cyber Security Risk Assessment
Practices**
Core Unified Risk Framework

Doctoral theses at NTNU, 2017:153

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

 **NTNU**
Norwegian University of
Science and Technology

 NTNU

 **NTNU**
Norwegian University of
Science and Technology

Gaute Bjørklund Wangen

Cyber Security Risk Assessment Practices

Core Unified Risk Framework

Thesis for the degree of Philosophiae Doctor

Gjøvik, June 2017

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication
Technology



Norwegian University of
Science and Technology

NTNU

Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

© Gaute Bjørklund Wangen

ISBN 978-82-326-2378-5 (printed version)

ISBN 978-82-326-2379-2 (electronic version)

ISSN 1503-8181

Doctoral theses at NTNU, 2017:153



Printed by Skipnes Kommunikasjon as

I dedicate this thesis to risky decisions and ground-shaking deadlifts.

Declaration of Authorship

I, Gaute Bjørklund Wangen, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

(Gaute Bjørklund Wangen)

Date:

Preface

Before you lies the thesis "Cyber Security Risk Assessment Practices: Core Unified Risk Framework," which is a compilation of my work on risk assessments in information security. The thesis has been written to fulfill the graduation requirements for the degree of Doctor of Philosophy in Information Security at the Norwegian University of Science and Technology (NTNU) in Gjøvik. I was engaged in researching and writing this thesis from April 2013 to February 2017. During my time at NTNU, I have been a part of the Management group at the Norwegian Center for Cyber and Information Security (CCIS), the Norwegian Laboratory for Information Security (NISLab), at the Department of Information Security and Communication Technology (IIK).

At the time of writing, the media reports new incidents caused by poor information security practices on a daily basis. Be it e-mail leakages, vulnerable SCADA systems, breached political parties, or third-parties escalating their privileges and causing trouble, it is all caused by poor security risk management practices. Security is often something that people consider at the end of a development project or post-deployment, when it is a lot more costly implement and, perhaps, too late. The evidence of this situation is everywhere in the market where there are plenty of solutions and applications that have a Swiss cheese security foundation and is a part of the weekly vulnerability-patching roll out event. Patching security vulnerabilities has even become such a commonplace event that I believe people have grown accustomed and consider it a necessary nuisance without questioning the premise. However, in a large part of these cases, poor and reactive security practices is the cause. For example, the need for profit is too big which makes the time to market too short and puts security in the backseat. A better approach to risk management will not solve all the problems in Cyber Security, however, gaining the upper-hand and becoming proactive in the security work is a big piece of the puzzle. Which is why this thesis focuses on risk assessment practices in information and cyber security.

I think that this thesis offers a balanced view on information security risk assessment practices. Hopefully, our proposals for new frameworks and models are realistic and have practical usefulness. We also contribute in answering some pressing questions within the research field and contribute to some additional problems.

I hope you enjoy reading this Thesis.

Gaute B. Wangen, 14.02.17.

Abstract

We conduct risk assessments to reducing the uncertainty regarding future events in order to make the best decisions possible and to control risk. In industry, the aim is to find the appropriate balance in risk-taking relative to the organization's risk appetite and tolerance. Too many security controls will inhibit business functionality, and the opposite will lead to unacceptable exposure. The complexity in the information and cyber security domain increases on a daily basis, which makes identifying, analyzing, and controlling the relevant risk events a major challenge. Thus, this thesis addresses several aspects of Cyber and Information Security Risk Assessment (ISRA) and Management (ISRM) Practices and contributes to novel research problems, methods, models, and knowledge within the discipline. This thesis applies the Design Science Research framework to investigate the theoretical and practical issues in ISRA.

The challenges within the ISRM field are many, and scholars, researchers, and practitioners have known about several of them throughout many years. With over hundred ISRA methods to choose from, multiple theoretical comparative studies of these methods, the literature on the topic of issues in ISRM was quite dispersed. To address this problem, this thesis applies literature review and structures the known research problems into a taxonomy. The findings from the initial literature survey were mainly theoretical, which made their practical relevance and implications uncertain. For a variety of reasons, one of the fundamental problems in information security is conducting empirical research. For validating and expanding the initial findings, this work reached industry practitioners through an online questionnaire. The study found that the main ISRM issues for the practitioners regarded risk communication, security measurements, and return on investments. While for risk assessment and analysis, we found the key issues to be the application of quantitative and qualitative methods, need for expertise, and asset evaluation.

Furthermore, empirical studies of method use are necessary to derive cause and effect between method choice, tasks, and results, and to figure out what works in ISRA. There exists multiple comparative assessments of ISRM/RA methods which are primarily scoped to compare method content to a predetermined set of criteria. Although the findings from applying these approaches are useful in understanding ISRA practices, they leave out the tasks and activities not present in the criteria and were not helpful in establishing cause and effect. To address this issue, we propose the Core Unified Risk Framework (CURF) as a bottom-up approach to ISRA method comparison and to measure completeness. By applying CURF, we found *ISO/IEC 27005 Information Security Risk Management* to be the most complete approach at present, with the *Factor Analysis of Information Risk (FAIR)* as the most complete risk estimation method. Also, we also discovered several gaps in the surveyed methods.

Moreover, we ran an experiment where we applied three different ISRA methods on four large-scale case studies. By using CURF in a novel way, it enabled us to do metadata analysis of ISRA reports and establish cause-effect between ISRA method choice and result. Our study found that the method selection influences the assessment process, along with its outcome.

Finally, one of the foremost discussed research problems in ISRM is the application of qualitative and quantitative methods. In short, the critique of the approaches is: (i) Quantitative ISRA is mostly conducted using previous cases and historical data. Depending on statisti-

cal data alone for risk assessments will be too naive as the data quickly becomes obsolete, lack of data, and is limited to only previously observed events, while the Qualitative ISRA is prone to several human biases. However, ISRM methods claim to be mainly quantitative or qualitative, but the quantitative versus qualitative risk situation is not strictly either-or. There are degrees of subjectivity and human-made assumptions in any risk assessment, and this work explores the intersection of these two approaches. Firstly, we analyzed the limitations of quantitative ISRA forecasting through a novel application of Taleb's Four Quadrants Risk Classification scheme. Using the findings from the prior CURF studies combined with the risk classification scheme, we construct a state of the art model for risk assessing a DDoS attack (Distributed Denial of service). The risk model consists of distinct classes and estimators gathered from CURF, where the novelty lies in the combination both the quantitative (statistics) and qualitative (subjective knowledge-based) aspects to model the attack and estimate the risk. The approach centers on qualitative estimations of assets, vulnerabilities, threats, controls, and associated outcomes, together with a statistical analysis of the risk. Our main contribution is the process to combine the qualitative and quantitative estimation methods for cyber security risks, together with an insight into which technical details and variables to consider when risk assessing the DDoS amplification attack.

Sammendrag

Risikovurderinger handler om å redusere usikkerhet vedrørende fremtidige hendelser for å ta så gode beslutninger som mulig og kontrollere risiko. Hvor målet å finne den riktige balansen i risikotaking i forhold til organisasjonens risikoappetitt og toleranse. For mange sikkerhetskontroller vil hemme virksomhetens funksjonalitet, og det motsatte vil føre til uakseptabel eksponering. Kompleksiteten i informasjons- og cybersikkerhet domene øker på daglig basis, noe som gjør arbeidet med å identifisere, analysere og kontrollere de relevante risikoene en stor utfordring. Denne oppgaven adresserer flere aspekter innen daglig praksis av Cyber - og informasjonssikkerhetsrisikovurdering (ISRA) og styring (ISRM). Oppgaven bidrar med nye problemstillinger, metoder, modeller og kunnskap i faget. Oppgaven anvender Design Science Research rammeverket for å undersøke de teoretiske og praktiske problemstillinger i ISRA. I tillegg til risikomodellering, metode sammenligning og valg.

Akademikere og praktikere har kjent til mange utfordringer innenfor ISRM feltet gjennom flere år. Disse problemstillingene har vært spredt i den akademiske litteraturen og det fantes ingen tilstrekkelig sammenstilling av dem. I tillegg har det blitt utviklet over ett hundre ISRA metoder å velge mellom med flere tilhørende komparative studier av disse metodene. For å løse dette problemet foretar denne avhandlingen en litteraturgjennomgang og strukturer de kjente problemstillinger i en taksonomi. Siden funnene fra den innledende litteraturstudien var innsamlet fra publisert materiale var det uklart hvor relevant disse funnene var en ISRA praktiker. Av en rekke årsaker er en av de grunnleggende problemene i informasjonssikkerhet å drive empirisk forskning, et hinder som vi har arbeidet med å overkomme. For å validere og utvide de første funnene benyttet vi elektronisk spørreskjema for nå bransjens praktikere. Studien fant at de viktigste ISRM problemene var risikokommunikasjon, sikkerhetsmålinger og å synliggjøre avkastning på investeringer. Mens for risikovurdering fant vi at de største utfordringene var bruk av kvantitative og kvalitative metoder, mangel på ekspertise, og verddivurdering.

Empiriske studier av ISRA metodebruk er nødvendig for å utlede årsak og virkning mellom metodevalg, prosess og resultater, og for å finne ut hva som fungerer. Det eksisterer flere sammenligningstilnæringer for vurdering av ISRM/RA, disse tilnærmingene har i hovedsak blitt utarbeidet for å sammenligne innholdet til et forhåndsbestemt sett av kriterier. Selv om funnene fra disse metodene er nyttig for å forstå ISRA praksis, så utelater de oppgaver og aktiviteter som ikke er til stede i de forhåndsbestemte kriteriene. Dette gjør at de ikke er nyttige til å etablere årsak og virkning. For å løse dette problemet, foreslår denne oppgaven "Core Unified Risk Framework (CURF)" som en bottom-up tilnærming til ISRA metode sammenligning og for å måle fullstendighet. Ved å bruke CURF, fant vi at *ISO/IEC 27005 Information Security Risk Management* var den mest komplette tilnærmingen, med *Factor Analysis of Information Risk (FAIR)* som den mest komplette risikoanalysemetoden. Dessuten oppdaget vi også flere svakheter i undersøkte metoder.

Videre kjørte vi et omfattende eksperiment der vi kjørte fire store case-studier hver med tre forskjellige ISRA metoder. Ved å bruke CURF på en innovativ måte gjorde det oss i stand til å gjøre metadata analyse av ISRA resultater og etablere årsak-virkning mellom metodevalg og resultat. Hvor vi fant at metodevalg påvirker både risikovurderingsprosessen sammen med innholdet og kvaliteten på resultatene. Som vi også nevnte innledningsvis, er en av de mest diskutert problemstillinger i ISRM anvendelsen av kvalitative

og kvantitative metoder. Kort sagt, så er kritikken av metodene følgende: (i) Kvantitativ ISRA er hovedsakelig utført ved bruk av tidligere saker og historiske data. Avhengig av statistiske data alene for risikovurderinger vil være for naivt ettersom data raskt blir foreldet, dataene er begrenset til observerte hendelser, og det er generelt mangel på statistikk vedrørende informasjonssikkerhetsrisiko. Mens Kvalitativ ISRA er sårbart for flere menneskelige psykologiske skjevheter i risikoforståelsen. Dagens situasjon er slik at ISRM metoder hevder å være hovedsakelig kvantitativ eller kvalitativ, men den kvantitative versus kvalitative risikosituasjon er strengt tatt ikke enten-eller. Ettersom det er grader av subjektivitet og menneskeskapte antagelser som underbygger alle risikovurderinger, og dette arbeidet utforsker også skjæringspunktet mellom disse to tilnærmingene. Vi analyserer begrensningene i kvantitativ ISRA prognoser gjennom å anvende Talebs risikoklassifiseringstilnærming hvor vi klassifiserer risiko basert på forutsigbarhet. Ved hjelp av funnene fra de tidligere CURF studiene kombinert med risikoklassifiseringsordningen, modellerer vi en kombinert kvalitativ og kvantitativ risikovurdering et DDoS-angrep (Distributed Denial of Service). Risikomodellen består av forskjellige klasser og estimatorer samlet fra CURE, hvor bidraget ligger i kombinasjonen både kvantitative (statistikk) og kvalitative (subjektiv kunnskapsbaserte) aspekter for å modellere angrepet og beregne risiko. Tilnærmingen fokuserer på kvalitative estimater for verdier, sårbarheter, trusler, kontroller og tilhørende resultater, sammen med en statistisk analyse av risikoen. Vårt viktigste bidrag er prosessen å kombinere kvalitative og kvantitative beregningsmetoder for cyber sikkerhetsrisikoer, sammen med en innsikt i hvilke tekniske detaljer og variabler en bør vurdere for et DDoS amplification angrep.

Acknowledgments

I have learned a lot during my time doing the Ph.D. at NTNU Gjøvik, formerly Gjøvik University College. I have many people to thank: First and foremost, Professor Einar Snekkenes for giving me the opportunity to do a Ph.D. and patiently discussing with me nearly every week. My co-supervisor and backup Professor, Stewart Kowalski for being knowledgeable and completely impossible to argue with, I appreciate the challenge. Nils Kalstad Svendsen for bringing me into the Risk Management course as a teaching assistant and, later, entrusting me with the course responsibility. Christoffer Vargtass Hallstensen and Stian Husemoen from IT Services and Digital Security for helping me during the Risk Management course work, and Christoffer for co-authoring some of my work. Andrii Shalaginov for patiently helping me with the statistics and the co-authorships. To my NTNU friends and colleagues Vasileios Gkioulos, Steven (Shao-Fang Wen), Edlira Martiri, Dimitra Anastasopoulou, Yi-Ching Liao, Vivek Agrawal, Roberto Rigolin Ferreira Lopes, Goitom Weldehawaryat, Håkon Gunleifsen, Ctirad Sousedik, Romina Muka, and others. I have enjoyed your company and thank you for the discussions and lunches. My old student colleagues for help and support during these years, especially Henry Johansen, Lars Arne Sand, Anders Sand Frogner, Roger Larsen, Anne Marie Dalen Øverhaug, and Ernst Kristian Henningsen.

We have also received external data for some of the research papers, in particular, I would like to thank Akamai Technologies and the Shadowserver Foundation.

The Bachelor groups I have supervised and classes I have taught which have made this a much richer experience. Especially Henrik, Niclas, and Erlend for proving that great things can be accomplished with the pedal to the metal and a large risk appetite.

I also thank my life partner, Ann Kristin Tøfte, for putting up with me, together with her continued support and interest in information security issues. My parents, sister, and brother for their support. Lastly, my children, Anna Sofie and Brage, for being a lot of fun and I trust that they will grow up to be better risk managers than their father.

Contents

I	Introductory Chapters	1
1	Introduction, motivation, and objectives	3
1.1	Information Security Risk Assessments	3
1.2	Research Problem and Motivation	4
1.3	Research Objectives, Questions, and Design	5
1.4	List of included publications	7
1.5	List of additional publications	7
1.6	Scope of the research	7
1.7	Thesis Outline	8
2	Background and Related Work	9
2.1	IT Governance and Information Security Management	9
2.2	Key Concepts in Information Security Risk Management	9
2.3	Risk Assessment	10
2.4	Risk Estimation and Analysis	10
2.5	Research on challenges in ISRM/RA	11
2.6	Comparison frameworks for ISRM/RA Approaches	13
2.7	Empirical comparisons of ISRM/RA	14
2.8	Cyber Security Risk Modeling	15
2.9	Summary of Related work	20
3	Research Method	21
3.1	Summary of Considered Research Methods	21
3.2	Applied Research Method	22
3.3	DSR Knowledge Contributions	25
4	Summary of Papers	27
4.1	A Taxonomy of Challenges in Information Security Risk Management [164]	27
4.2	A Comparison between Business Process Management and Information Security Management [165]	29
4.3	An Initial Insight Into InfoSec Risk Management Practices [157]	30
4.4	An Initial Insight Into Information Security Risk Assessment Practices [159]	30
4.5	A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF [161]	31
4.6	Information Security Risk Assessment: A Method Comparison [160]	33
4.7	Quantitative Risk, Statistical Methods, and The Four Quadrants for Information Security [162]	34
4.8	Cyber Security Risk Assessment of a DDoS Attack [163]	34
5	Summary of Thesis Contributions	37
5.1	Theoretical Insights into ISRM Practices	37
5.2	New Practical Insights into ISRA practices	37
5.3	The Core Unified Risk Framework (CURF)	38
5.4	CURF Applications	38

CONTENTS

5.5	Evaluation of Artifacts	39
5.6	Summary of Contributions within the DSR Quadrants	40
6	Future Work	43
6.1	Future directions for CURF	43
6.2	New research area in method comparison	43
6.3	Opportunities in risk prediction and modeling	44
6.4	Future directions in generic ISRM/ISRA	45
7	Conclusion	47
II	Published Research Papers	49
8	Article I - A Taxonomy of Challenges in Information Security Risk Management	51
8.1	Abstract	51
8.2	Introduction	51
8.3	Related Work	52
8.4	A Taxonomy of Challenges	52
8.5	Analysis and Discussion	58
8.6	Conclusion	59
9	Article II - A Comparison between Business Process Management and Information Security Management	61
9.1	Abstract	61
9.2	Introduction	61
9.3	Related Work	63
9.4	IT Governance, Information Security Risk & Management	63
9.5	Business Process Modelling and Management	66
9.6	Method	69
9.7	A Comparison of ISM and BPM Lifecycles	69
9.8	A Comparison of Organizational Views	70
9.9	A comparison of ISM and BPM domains	73
9.10	Conclusion	75
10	Article III - An Initial Insight Into InfoSec Risk Management Practices	77
10.1	Abstract	77
10.2	Introduction	77
10.3	Research Method	78
10.4	Results	80
10.5	Discussion	85
10.6	Conclusion	87
10.7	Erratum	89
11	Article IV - An Initial Insight Into Information Security Risk Assessment Practices	91
11.1	Abstract	91
11.2	Introduction	91
11.3	Research Method	92
11.4	InfoSec Risk Assessment practices	95
11.5	Risk Analysis Practices	97
11.6	Choosing Risk Treatment Strategies	106
11.7	Summary & Conclusion	107

12 Article V - A framework for estimating information security risk assessment method completeness - Core Unified Risk Framework, CURF	111
12.1 Abstract	111
12.2 Introduction	111
12.3 Reviewed Methods	112
12.4 Framework development	114
12.5 Core Unified Risk Framework (CURF)	116
12.6 ISRA Method Completeness	122
12.7 Scope and Limitations of the current ISRA methods	126
12.8 Relationship to other literature	128
12.9 Conclusions	130
13 Article VI - Information Security Risk Assessment: A Method Comparison	133
13.1 Abstract	133
13.2 Introduction	133
13.3 Background and Related Work	134
13.4 Method	136
13.5 Experiences using the ISRA methods	137
13.6 Analysis and Discussion	139
13.7 Conclusion	142
14 Article VII - Quantitative Risk, Statistical methods, and the Four Quadrants for Information Security	145
14.1 Abstract	145
14.2 Introduction	145
14.3 Information Security and Risk Assessment	146
14.4 Methodology for statistical risk analysis and classification of events	148
14.5 Case Studies	149
14.6 Discussion	155
14.7 Conclusion & Future work	156
15 Article VIII - Cyber Security Risk Assessment of a DDoS Attack	159
15.1 Introduction to InfoSec Risk Assessment	159
15.2 Choice of Methods	161
15.3 Case Study: Qualitative Risk Assessment of a DDoS attack	164
15.4 Quantitative Risk Analysis	168
15.5 Discussion & Conclusion	171
Bibliography	175

List of Figures

1.1	The ISO/IEC 27005:2011 Information Security Risk Management process	4
1.2	Research Flow, Research Questions, and published Papers	6
2.1	A CORAS model of an access control risk [149].	16
2.2	The development of bandwidth consumption (Gbps) of DDoS-attacks during the last 15 years. <i>Data source: Arbor Networks and media reports</i>	18
2.3	Malware development from 1984-2017. Source: AVTest - The Independent IT-Security Institute (https://www.av-test.org). <i>Reprinted with permission</i>	19
2.4	Taleb's four quadrants for Risk Classification. <i>Based on Taleb[143]</i>	19
3.1	Research phases together with a summary of applied methods, RQs, and published articles	22
3.2	DSR Knowledge Contribution Framework based on Gregory & Hevner [68]	25
4.1	Relationship between Research Papers.	27
4.2	Classification scheme in the Taxonomy of Challenges for ISRM	28
4.3	Summary of BPM-ISM and ISM-BPM comparison. Legend: - "X" marks how the ISM domains are covered and can be implemented in the BPM domains. "0" marks which ISM domains support BPM domains and where.	29
4.4	Top level of CURF. The generic output of the Risk Evaluation is prioritized risks.	32
4.5	The Four Quadrants with Risk Classifications. <i>Based on Taleb[143]</i>	35
4.6	Histogram of DDoS magnitudes and durations with normal curve, without two largest outliers. <i>Data Source: Akamai [19]</i>	35
4.7	Expanded Event Tree also including subjective estimates of threat actors and control efficiency.	36
5.1	DSR Knowledge Contribution Matrix for this Thesis	41
8.1	The Taxonomy of Challenges in ISRM	53
9.1	Example of a Business Process Hierarchy.	62
9.2	Plan Do Check Act-phases of ISMS implementation as described in ISO/IEC 27000:2009[10].	64
9.3	Connection between Mission, Vision, Strategy and Business Processes. <i>Based on Mahal[106]</i>	67
9.4	Illustration of Guides and Enablers that contribute to the BP. <i>Based on [106, 40]</i>	68
9.5	Illustration of common BPM & ISM Level 1 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.	71
9.6	Illustration of common BPM & ISM Level 2 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.	72
9.7	The illustration shows how the IS Incident Management control can be modelled within the BP domain.	73

LIST OF FIGURES

9.8	Heatmap indicating how well ISM covers the BPM domains, green signals no issues, red signals significant issues.	76
10.1	How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)	78
10.2	Respondent demographics, based on company size (x-axis), industry (Y-axis) and Continent.	80
10.3	Overview of Erratum	89
11.1	How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)	93
11.2	Respondent demographics, based on company size (x-axis), industry (Y-axis) and Continent.	94
11.3	ISRA practices on different organizational tiers	95
11.4	Statements and rankings regarding Assets (Scale 1 - <i>Strongly disagree</i> to 6 - <i>Strongly agree</i>)	100
11.5	Results from opting to reduce either probability or consequence	108
12.1	The ISO/IEC 27005:2011 ISRM process, the <i>Risk Assessment</i> activities mark the scope of this paper.	113
12.2	CURF development process	116
12.3	Top level of CURF. The generic output of the Risk Evaluation is prioritized risks.	116
14.1	Example of potential outcomes from an APT/Espionage attack, Y=Consequence X=Time. The initial shock comes from detecting and responding to the breach. The long-term C is represented as a Logistic function, where P of all A are bound with a close to unsolvable U.	151
14.2	Gameover Zeus infection probability distribution and timeline. Right shows results of Q-Q plot of LogNormal distribution. Data source: The Shadowserver Foundation.	152
14.3	Comparison of the original DDOS data and modeled distribution	154
14.4	Factors leading into the Fourth Quadrant. <i>Pictures reprinted with permission, from Audestad, 2009 [26]</i>	155
14.5	The Four Quadrants with Risk Classifications. <i>Based on Taleb[143]</i>	157
15.1	The development of bandwidth consumption (Gbps) of DDoS-attacks during the last 15 years. <i>Data source: Arbor Networks and media reports</i>	160
15.2	Illustration of Network robustness with an absorbed amplification attack. Network capacity at 10 Gbps, everything above constitutes a DoS.	165
15.3	Fitting DDoS Magnitude and Duration data set by means of Q-Q Plot using γ -distribution. Two outliers are evident at the high end of the range for both distributions.	169
15.4	Histogram of DDoS magnitudes and durations with normal curve, without two largest outliers. <i>Data Source: Akamai [19]</i>	170
15.5	Bubble plot of the attack bandwidth depending on the duration for each scenario. Size of the bubble also denote magnitude of the attack. Scenarios are depicted with different colours.	171
15.6	Event Tree displaying probability of monthly DDoS occurrence for the Case study.172	
15.7	Expanded Event Tree also including subjective estimates of threat actors and control efficiency.	173

List of Tables

2.1	Overview of Risk Analysis approaches. <i>Adapted from Aven [33]</i>	10
2.2	Overview of a set of existing methods with categorization and descriptions	12
4.1	Perceived contributions of the ISRM program to different areas	30
4.2	Comparison of observable theoretical differences from CURF and differences in reports	33
5.1	Evaluation of Artifacts	39
9.1	A Comparison of the generic PDCA steps and the BPM Lifecycle	69
9.2	A comparison of organizational views from the NIST SP 800-39[103] and BPM Methodology Framework[70, 106, 1]	71
9.3	Summary of BPM-ISM and ISM-BPM comparison. Legend: - "X" marks how the ISM domains are covered and can be implemented in the BPM domains. - "0" marks which ISM domains support BPM domains and where.	74
10.1	Groups and Forums where the questionnaire was posted	79
10.2	Classification of Respondents, total 46.	80
10.3	Results from asking "Which definition best describes an InfoSec Risk in your opinion?"	81
10.4	Answers to "Our ISRM program is ran by our IT department" sorted by company size.	81
10.5	Differences in application of industry standards for ISRM program development	82
10.6	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.	83
10.7	Perceived contributions of the ISRM program to different areas	83
10.8	Observable differences between categories from ISRM contributions	84
11.1	Groups and Forums where the questionnaire was posted	93
11.2	Classification of Respondents, total 46.	94
11.3	Roles attending in risk assessments.	97
11.4	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)	97
11.5	Views on importance of knowledge areas for ISRA. (1 - <i>Not Important</i> to 6 - <i>Very Important</i>	98
11.6	Notable differences on Knowledge areas between Expertise groups	98
11.7	Practitioner view on issues related to assets. (Scale 1 - Strongly disagree, 6 - Strongly agree)	99
11.8	Statistically significant and notable differences between expertise categories on assets	100
11.9	Descriptive statistics of ISRA statements. (1 - Strongly Disagree, 6 - Strongly Agree)	101

LIST OF TABLES

11.10 Distribution of answers (x-axis) regarding ISRA statements (y-axis). Statement numbers correlate with descriptions in Table 11.9. (1 - Strongly Disagree, 6 - Strongly Agree) 101

11.11 Notable difference between categories (Full statements correspond to numbers in Table 11.9) 103

11.12 Correlations between ISRA statements. (Full statements correspond to numbers in Table 11.9) 104

11.13 Application of tools, methods, and concepts in ISRA. (Scale: 1 - Unfamiliar, 2 - Very Seldom, 3 - Seldom, 4 - Sometimes, 5 - Often, 6 - Very Often) 105

11.14 Views on importance of tasks and items for Risk Analysis. (Scale: 1 - Not important, 6 - Very important) 106

11.15 Rank the phases of the ISRA process according to your perceived importance, scale 1 (not important) - 6 (very high importance) 106

11.16 Respondents' recommendation of risk treatment options in ISRA. Scale 1 (Never) to 6 (Very often) 107

12.1 Risk Identification process and output comparison. Scores: XX=2, X=1. Max=22 per row and Max=50 per column 119

12.2 Risk Estimation processes and output comparison. Scores: XX=2, X=1, -=0. Scores Max=22 per row and Max=46 per column 121

12.3 Risk Evaluation processes and output comparison. Scores: XX=2, X=1, -=0. Scores Max=22 per row and Max=6 per column 122

12.4 Method process completeness according to comparison criteria according to previous scores. 122

13.1 CURF, main qualitative differences between frameworks 135

13.2 Summary of reported advantages, disadvantages, and needs covered with supporting literature from each method 139

13.3 Observable differences in the risk assessment reports. Max score 8 per method, 24 per row, and with 26 identified tasks, and 208 per column. 140

13.4 Comparison of observable theoretical differences from CURF and differences in reports. XX=Addressed, X=Partially addressed, & 0=Not addressed 141

14.1 Example of DDoS attack magnitude distributions and probabilities, with conditional probabilities of semi-annual occurrence. 153

14.2 Confidence Intervals for defined % of the DDOS attacks to be eliminated 154

15.1 Asset considerations for the DDoS attack 165

15.2 Examples of approximate amplifications by exploiting vulnerable UDP, including possible amplification of the 100 Mbps connection. *Data source: Hilden [76], Norwegian Security Authority (NSM)* 167

15.3 Threat assessment for DDoS attack, *K* represents confidence in the estimates . . . 167

15.4 Control efficiency estimation. *K* represents confidence in the estimates 168

15.5 Frequencies of DDoS Magnitude observations from Akamai Dataset [19]. 169

15.6 Frequencies for the defined events, *A*. *Data Source: Akamai [19]* 170

15.7 Overview attack severity for the case study and duration frequencies. *Data Source: Akamai [19]* 171

List of Abbreviations and Definitions

Abbreviations:

A	Event (in Risk Analysis)
ADM	Application Domain Maturity
ALE	Annual Loss Expectancy
ANOVA	Analysis of Variance
APT	Advanced Persistent Threats
BP	Business Proces
BPM	Business Process Management/Modeling
C	Consequence (in Risk Analysis)
CERT	Computer Emergency Response Team
CIRA	Conflicting Incentives Risk Analysis
CORAS	UML Model-based method for security risk analysis
CharGen	Character generator protocol
CI	Confidence Interval
CIA	Confidentiality, Integrity, and Availability
CRAMM	CCTA Risk Analysis and Management Method
CRDF	Cloud Risk Decision Framework
CURF	Core Unified Risk Framework
CySeMoL	Cyber Security Modeling Language
DoS	Denial of Service
DDoS attack	Distributed Denial of Service
DSR	Design Science Research
ERM	Enterprise Risk Management
FAIR	Factor Analysis for Information Risk
Gbps	Giga bits per second
ICT	Information and Communications Technology
IT	Information Technology
InfoSec	Information Security
IS	Information Security
ISM	Information Security Management
ISMS	Information Security Management System
ISACA	Information Systems Audit and Control Association
ISO	International Standardization Organization
ISP	Internet Service Provider
ISO27005	ISO/IEC 27005:2011 Information technology, Security techniques, Information security risk management
ISRA	Information Security Risk Assessment
ISRAn	Information Security Risk Analysis
ISRM	Information Security Risk Management
K	Knowledge (in Risk Analysis)
MCRDF	Microsoft Cloud Risk Decision Framework
NSM	Norsk Sikkerhetsmyndighet / Norwegian Security Authority
NSMROS	Norwegian National Security Authority Risk and Vulnerability Assessment

LIST OF TABLES

OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OA	OCTAVE Allegro
P	Probability (in Risk Analysis)
PDCA	Plan-Do-Check-Act
PRA	Probabilistic Risk Analysis
R	Risk (in Risk Analysis)
RA	Risk Analysis
RAIS	Norwegian Data Protection Authority (Datatilsynet) Risk Assessment of Information Systems
RM	Risk Management
ROSI	Return On Security Investments
RQ	Research Question
S	Sensitivity (in Risk Analysis)
SDLC	Software Development Life Cycle
SLE	Single Loss Expectancy
SoM	Solution Maturity
SPoF	Single Point of Failure
U	Uncertainty (in Risk Analysis)
UDP	User Datagram Protocol
UML	Unified Modeling Language

Definitions:

Frequentist / Quantitative Probability	<i>The fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed [29]</i>
Hybrid risk assessment	Combined qualitative and quantitative risk assessment model 1. The Effect of Uncertainty on Objectives[15, 16] 2. $R = f(A, C, U, P, S, K)$ [28]
Risk	3. The potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization [15] Note 6 to entry.
Risk Analysis	The systematic use of information to identify sources to estimate the risk [11]
Risk Assessment	Consists of the overall process of risk analysis and risk evaluation [15]
Risk Evaluation	<i>The process of comparing the estimated risk against given risk criteria to determine the significance of the risk [11]</i>
Risk Management	A set of activities and methods applied in an organization to manage and control the many risks that can influence achievement of business goals [16]
Subjective Knowledge-based Qualitative Probability	The assessor's uncertainty (degree of belief) of the occurrence of an event[29]

Part I

Introductory Chapters

Introduction, motivation, and objectives

This chapter gives an introduction to the research field, before presenting the reader with the problem description, motivation and research questions. Further, we provide an overview of the research publications and how they coincide with the research flow and questions. Lastly, we outline the remainder of the Thesis.

1.1 Information Security Risk Assessments

Achieving information security (InfoSec) is a difficult task, one that is constantly evolving and is likely never to be fully overcome or understood. Best practice InfoSec depends heavily on the risk management process [13, 36, 155], which is in itself a complicated matter and the topic of this Thesis. With the development of technology throughout the last decades, InfoSec risk management (ISRM) has increasingly become more critical in the day to day operations as it is crucial in determining what to protect and how to invest in security. InfoSec risk comes from applying technology to information [36], where the risks revolve around securing the confidentiality, integrity, and availability of information [13]. ISRM is the process of managing these risks, and, to be more specific; the practice of continuously identifying, reviewing, treating and monitoring risks to achieve risk acceptance [15], the ISRM process is illustrated in Figure 1.1. We conduct InfoSec risk assessments (ISRA) to make the best possible decision regarding future activities and to control risk. The risk assessment process consists of gathering relevant information, analyzing, and evaluating, to obtain the best possible decision basis regarding planned activities. As most organizations operate on a limited security budget, it goes without saying that having a well-functioning ISRM process is beneficial, both regarding security level and economy.

There are several approaches to ISRA and many practices for conducting an assessment [127], however, most ISRA approaches agree that asset, threat, and vulnerability are the key components of the information security risk [161]. An asset being something of value to the organization, often regarding information. In practice, we identify assets within the scope of the assessment and evaluate them according to value and criticality. A threat is an opponent that is in a position to trigger an adverse action, besides mother nature, this opponent is always a person. Vulnerabilities are points of weakness in the system that a threat can exploit to gain access to the asset. Weaknesses can, for example, be inherent in a piece of software, introduced through misconfiguration, or human negligence. Further, by analyzing these three, often in conjunction, the assessor identifies adverse events and produces a risk estimate with the associated consequence(s) and rates of occurrence. The decision-maker uses this estimate to determine whether a risk is acceptable or not. If a risk is found unacceptable, the organization has to consider implementing risk treatments; either by mitigation, avoidance, or transference to a another party. In some cases, the risk itself may be unacceptable, but the risk treatment cost can be so high or have such a low return on investment that the decision-maker may choose to retain the risk.

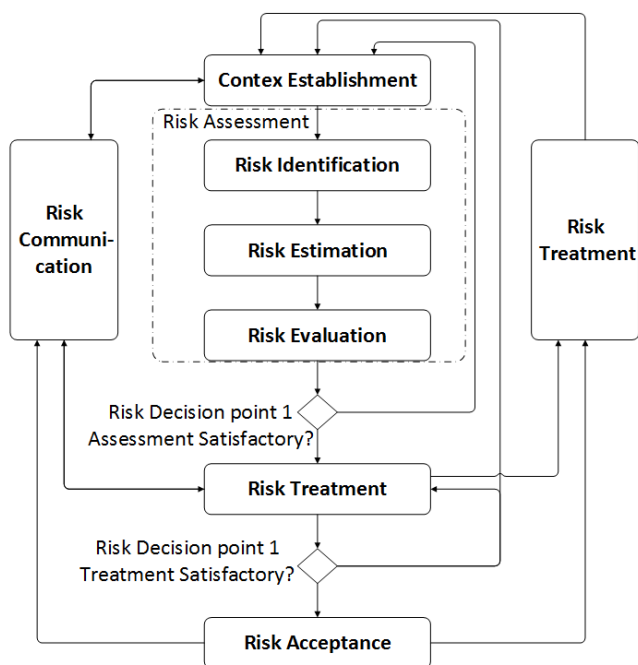


Figure 1.1: The ISO/IEC 27005:2011 Information Security Risk Management process [15]

1.2 Research Problem and Motivation

The challenges within the ISRM field are many [58, 133, 130] and several of them have been known to scholars, researchers, and practitioners throughout many years. With over hundred methods to choose from [127], multiple theoretical comparative studies of these methods [2, 38, 142, 126, 44, 127, 17], and research problems in ISRA [58, 130, 133, 36], we consider the theoretical side of ISRA as a well-saturated research area. Whereas most of the sources come from published academic literature, the practical aspects of ISRA remain relatively unexplored by scholars. Over ten years ago, Kotulic and Clark [97] argued that *"Information security research is one of the most intrusive types of organization research, and there is undoubtedly a general mistrust of any "outsider" attempting to gain data about the actions of the security practitioner community."* This argument may still hold true, although there has been published empirical studies on information security issues since the Kotulic and Clark study (e.g. [39, 86, 115, 43]), there is still a gap regarding ISRA practices.

Sufficient to say, ISRM as a research field presents several interesting research problems. In order to address any of these problems, the underlying reasons must be well understood for the scientific community and industry to be able to make progress. Simply addressing one isolated problem at a time while being uninformed of the remaining challenges is not enough, as the ISRM is a complex and interconnected research field. Thus, there is a need for an understanding of both the theoretical and practical problems in ISRM.

Furthermore, regarding ISRA practices, there are many different definitions of risk [29] and many unique ISRA approaches [127]. This situation has likely occurred due to ISRA practices varying between industries, disciplines, and organization. As mentioned, there exists multiple comparative assessments of ISRM/RA methods. However, these are primarily

scoped to compare method content to a predetermined set of criteria. Although findings from applying these approaches are useful in understanding ISRA practices, they leave out the tasks and activities not present in the criteria. In order to figure out what works in ISRM, there is a need for mapping all activities and tasks present in each method to obtain a holistic understanding of day to day practices, in addition to a comprehensive comparison base on each method to study cause-effect. To our knowledge, there has not been conducted any studies on how the choice ISRA method affects the results. Empirical studies of method application are needed to derive cause and effect between method choice, tasks, and results.

Finally, one of the foremost discussed research problems in ISRM is the application of qualitative [128, 80, 132, 131, 42] and quantitative [71, 80, 82, 62, 36] methods. In short, the critique of the approaches is: (i) Quantitative ISRA is mostly conducted using previous cases and historical data. Depending on statistical data alone for risk assessments will be too naive as the data quickly becomes obsolete [26], lack of data [68], and is limited to only previously observed events [144]. While the Qualitative ISRA is prone to several biases [89, 144, 132, 131]. ISRM methods claim to be mainly quantitative [36, 62] or qualitative [46, 37, 53], but the quantitative versus qualitative risk situation is not strictly either-or. There are degrees of subjectivity and human-made assumptions in any risk assessment, and the intersection of these two approaches (hybrid) remains largely unexplored.

1.3 Research Objectives, Questions, and Design

This Thesis aims to accomplish the following objectives: First, establish a theoretical foundation for the study regarding established ISRA methods and known both practical and theoretical challenges. Second, validate these problems with a selection of the practitioner community to determine where the need for progress is most pressing. Third, develop a solution to address the identified problem(s), and, lastly, validate and improve our proposed model. Figure 1.2 summarizes the flow of research and approach to research questions. Following are the research questions (RQ) with corresponding descriptions:

- **Question 1: What are the known theoretical issues in Information Security Risk Management?**
There exist multiple sources on ISRA practices published by scholars, researchers, and practitioners working with relevant problems [58, 133, 130]. However, there were no taxonomies or frameworks for classifying and comprehensively mapping the known ISRM problems. A firm grasp on the state-of-the-art is necessary to address the most pressing issues within the research field. RQ 1 investigates the known theoretical challenges through literature review and provides the basis for further studies in the field.
- **Question 2: How does the overall Information Security Management Frameworks compare with other Business Management frameworks?**
From our literature review, we found multiple studies of InfoSec risk management and assessment standards, methods, and frameworks being compared among themselves. However, there were no studies of InfoSec management literature to other management literature. Thus, This research question examines a selection of the InfoSec management standards with other management frameworks, and investigates the similarities and differences between them, explore possible integration, and analyze the theoretical issues. Since ISO27005 [15] suggests business processes as one out of two primary assets, we chose to compare with frameworks for *Business Process Management*.
- **Question 3: How do the theoretical ISRA issues coincide with practical challenges in Information Security Risk Management?**

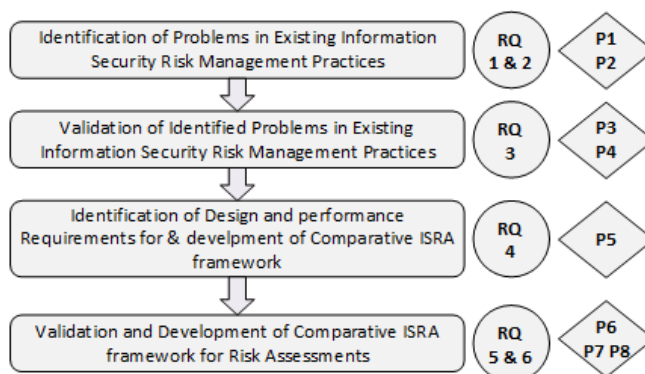


Figure 1.2: Research Flow, Research Questions, and published Papers

This study investigates the practitioner's view of the previously discovered issues and challenges within ISRA. The literature is scarce regarding the current ISRA industry practices and issues from the practitioner's point of view. This research question explores the ISRA industry's opinions on the main ISRM issues.

- **Question 4: How do different ISRA approaches compare qualitatively from a bottom-up perspective?**

When we were working on the way to derive how the various ISRA methods handle specific issues, our initial work showed that there exists a lot of ISRM/RA comparison purposes. However, all apply an individual set of pre-defined criteria which were equivalent to a top-down static comparison and would not reveal differences beyond these criteria. This research question explores how to compare ISRA methods with a qualitative bottom-up approach. We propose a model to reveal all differences and how each method handles specific issues found in the previous studies.

- **Question 5: How does the choice of ISRA method matter for the risk assessment results?**

While the proposed model from answering RQ 4 enabled us to compare ISRA methods on a theoretical basis, RQ 5 further validates the proposed model and explores the application of the method for case study comparison. Further, RQ 5 examines how each of the three applied ISRA methods handle issues. Further, RQ 5 explores the differences in experience and results from using the three methods, and aims to establish cause and effect between ISRA method content and produced risk assessments.

- **Question 6: What are the requirements and limitations for constructing a hybrid risk assessment model?**

The application of the statistical method and risk quantification is one of the most heavily discussed problems in ISRM and was also highlighted in our initial research. More mature sciences, such as engineering and medical, generally prefer risk assessments based on statistical methods, but the qualitative approach dominates in InfoSec. Thus, RQ 6 explores the limitations of quantitative risk assessment methods for information security, before proposing a combined quantitative and qualitative (*hybrid*) ISRA model by applying the model developed in answering RQ 4 and exploring the utility of the hybrid approach.

1.4 List of included publications

1. **Article I [164]:** Wangen, Gaute & Snekkenes, Einar. A Taxonomy of Challenges in Information Security Risk Management. Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskoneranse - NISK 2013 - Stavanger, Akademika forlag, 2013, 2013.
2. **Article II [165]:** Wangen, Gaute & Snekkenes, Einar. M. Ganzha L. Maciaszek, M. P. (Ed.) A Comparison between Business Process Management and Information Security Management. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FEDCSIS), IEEE, 2014, 2, 901-910.
3. **Article III [157]:** Wangen, Gaute. An Initial Insight Into InfoSec Risk Management Practices. Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskoneranse - NISK 2015 - Ålesund, Open Journal Systems, 2015, 2015.
4. **Article IV [159]:** Wangen, Gaute. Ganzha, M.; Maciaszek, L. & Paprzycki, M. (Eds.) An initial insight into Information Security Risk Assessment practices Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, IEEE, 2016, 8, 999-1008.
5. **Article V [161]:** Wangen, Gaute; Hallstensen, Christoffer & Snekkenes, Einar. Framework for estimating information security risk assessment method completeness - Core Unified Risk Framework, *Submitted Manuscript in 2015 to the Springer International Journal of Information Security*.
6. **Article VI [160]:** Wangen, Gaute. Information Security Risk Assessment: A Method Comparison. Forthcoming IEEE Computer Special Issue on Security Risk Assessments, 2017.
7. **Article VII [162]:** Wangen, Gaute & Shalaginov, Andrii. Lambrinouidakis, C. & Gabilon, A. (Eds.). Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers, Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security, Springer International Publishing, 2016, 127-143
8. **Article VIII [163]:** Wangen, Gaute; Shalaginov, Andrii & Hallstensen, Christoffer. Cyber Security Risk Assessment of a DDoS Attack International Conference on Information Security, 2016, Springer International Publishing, 183-202

1.5 List of additional publications

1. **Article IX [158]:** Wangen, Gaute. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, 2015, 6.2: 183-211.
2. **Article X [156]:** Wangen, Gaute. Conflicting Incentives Risk Analysis: A Case Study of the Normative Peer Review Process. *Administrative Sciences*, 2015, 5.3: 125-147.

1.6 Scope of the research

The main scope of this research is ISRM, in particular, ISRA practices and application. General InfoSec literature is partially in scope where ISRM problems have been traced back to more fundamental problems in InfoSec. Considering the ISRM process, illustrated in Figure 1.1, this work is primarily limited to risk assessments and associated processes, including risk identification, estimation, and evaluation. The intended audience of this project

is InfoSec professionals and academics, together with other ISRM practitioners and stakeholders.

1.7 Thesis Outline

This thesis consists of two parts, whereas Part I contains the overview of the research project, and Part II consists of the research papers. In Part I, the background and the related work are presented in Chapter 2, in which we provide the reader with the fundamental theory necessary for understanding this thesis. Chapter 3 contains a description and discussion of the scientific research methods applied in this project, in particular, Design Science Research (DSR) and how the presented work fits this paradigm. Chapter 4 contains a summary of the eight research papers, while Chapter 5 summarizes the key contributions from the research project. While Chapter 6 introduces potential topics and directions for future work, and Chapter 7 concludes the work.

In Part II, Chapters 8-15 include the eight research papers that constitute the main part of the thesis. The papers are presented in the same sequence as in Section 1.4.

Background and Related Work

This chapter has two parts: (i) Presents a summary of the key concepts that are fundamental to understanding this Thesis, (ii) Explores the related work within the research area. Part I starts with an explanation of the main top-level concepts within information security, such as InfoSec Management (ISM) and governance. Then, moves on to define and explain the ISRM process, risk assessment, and risk analysis. Part II discusses previous work on research challenges in InfoSec, ISRM/RA comparison frameworks, empirical ISRM studies, and InfoSec risk modeling. Lastly, we summarize the identified gaps in the reviewed work and position the Thesis.

2.1 IT Governance and Information Security Management

Gregory [68] writes that *"The purpose of IT governance is to align the IT-organization with the needs of the business"*. The discipline involves a series of activities to accomplish this goal such as creating IT-policy, internal prioritizing between and alignment of mission, objectives and goals, program and project management. Security governance is the organization's strategy or plan for managing security risks at an acceptable level. ISO/IEC 27001[13] is a renowned standard for information security management (ISM). There exists a large body of literature related to ISM, in addition to current standards, there are several books on the subject [168, 5, 167, 64]. The primary goal of InfoSec is to secure the business against threats and ensure success in daily operations[11] by ensuring confidentiality, integrity, availability, and non-repudiation. Information can be present in many forms of the organization, people may store it on a physical medium, on paper, or it can be an employee's knowledge and experience. Common for all these is that they are all valuable assets to an organization and their security needs to be ensured. The main component of ISM is to establish a security program, often referred to as an information security management system (ISMS). The purpose of the ISMS is to ensure confidentiality, integrity, and availability of the organization, assured by choosing and implementing the appropriate security measures and controls. These measures can be chosen from the ISO/IEC 27002 [61], which is a specialized standard consisting of security measures and how to implement them and is used to determine which measures and controls are appropriate, which makes ISRM a cornerstone in ISM.

2.2 Key Concepts in Information Security Risk Management

All organizations perform InfoSec risk management in some form, although it may not be formalized in policy. For example, someone locking files into a cabinet or locking his computer screen are managing risks. Although mature organizations often obtain higher levels of InfoSec by formalizing and implementing an ISMS, where one of the main components of an ISMS is managing IT risks[60]. The ISO standard *Risk Management - principles and guidelines* (31000:2009)[16] is one of the cornerstones of risk management and is a general standard that applies to a wide range of businesses. ISO 31000 defines risk as *the effect of uncertainty on objectives*. Using the same standard, *Risk management* can be understood as a set of activities and methods applied in an organization to manage and control the

2. BACKGROUND AND RELATED WORK

many risks that can influence the achievement of business goals. ISO/IEC 27005:2011 is a standard specialized for ISRM and defines the formal process of managing risks as an iterative process of reviewing and monitoring risks, see Figure 1.1. The ISRM process includes context establishment, risk assessment, communication and treatment to obtain risk acceptance[15]. Risks for information systems are generally analyzed by using a probabilistic risk analysis (PRA), where impact to the organization (e.g. financial loss if a risk occurred) with a corresponding probability calculation of occurrence. Using the results of the analysis, the risks are assessed, and if the risk is found unacceptable, steps are taken to mitigate the risk to the organization which consists of choosing a strategy and measures for controlling undesirable events.

2.3 Risk Assessment

At its core, risk assessment is about reducing uncertainty regarding future events. There exist several definitions of IS risk, for explanatory purposes we found the ISO/IEC 27000:2014, Note 6 to entry definition most comprehensive [11]: *"potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization"*. The provided definition works well because it includes assets, vulnerabilities, and threats and explains their logical connection. In addition to existing controls and barriers, these are the key components in the risk assessment. These key elements are what we investigate to reduce uncertainty regarding an identified risk and to derive consequences with associated probabilities. An ISRA is the *overall process of risk analysis and risk evaluation*[11], and risk analysis is the *systematic use of information to identify sources to estimate the risk*[11]. Risk evaluation is the *"process of comparing the estimated risk against given risk criteria to determine the significance of the risk"*[11].

Risk analysis consists of two steps; risk identification and risk estimation. Risk identification can be conducted in several ways, such as brainstorming on threats and vulnerabilities to significant assets or through the use of historical incident data. There also exists specific tools to aid in threat and vulnerability discovery such as Annexes C and D in ISO/IEC 27005 [15], The Vulnerability Assessment & Mitigation Methodology (VAM) [23], and penetration tests which are an example of a technical vulnerability assessment.

Table 2.1: Overview of Risk Analysis approaches. *Adapted from Aven [33]*

Main Category	Procedure	Description
Simplified Risk Analysis	Qualitative	A simplified RA is an informal approach that maps the risk profile using brainstorming and group discussions. The identified risks from this method are usually projected using a qualitative risk matrix, e.g. consisting of high, medium, low values.
Standard Risk Analysis	Qualitative or Quantitative	A more formal approach to RA, where renowned RA methods are used. Risk Matrices are often applied to project the results.
Model-based Risk Analysis	Primarily Quantitative	Model-based Risk Analysis uses techniques such as fault-tree analysis and event-tree analysis to

2.4 Risk Estimation and Analysis

A significant amount of the renowned ISRM frameworks recommends probabilistic risk analysis (PRA) for risk estimation. In their paper, Kaplan and Garrick [90] proposed the *set of triplets* for PRA consisting of *Scenario, Likelihood, and Consequences*. For InfoSec we can define the scenario as a combination of assets, vulnerability, threat, controls, and outcome [15]. Where each step in the approach generates useful knowledge in on its own, for example, a thorough threat assessment will provide information regarding opponents that are

also useful in other risk-related activities and decision-making. The combination of these activities leads to the identified risk scenario or *event*, in which the risk assessor estimates the probability and impact. Aven [29] defines two basic approaches to risk estimation: (i) the frequentist (quantitative) - "*the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed*". Quantitative models typically apply statistical models, historical data, and simulations to produce numerical risk estimates. (ii) The subjective knowledge-based probability (qualitative) - "*assessor's uncertainty (degree of belief) of the occurrence of an event*". The subjective approach is reliant on expert subjective knowledge for predictions, where risk estimates are expressed with words rather than numbers. Table 2.1 shows an overview of the applications of the qualitative and quantitative approaches with associated descriptions. There exist critiques of both approaches, for example, depending on statistical data (quantitative) alone for risk assessments will be too naive as the data quickly become obsolete [26] and is limited to only previously observed events [144]. While the subjective (qualitative) risk assessment is prone to several biases [89] (Part II) [144]. ISRM methods claim to be mainly quantitative [36, 62] or qualitative [46], however, the quantitative versus qualitative risk situation is not strictly either-or. There are degrees of subjectivity and human-made assumptions in any risk assessment. The effort to combine the qualitative and quantitative approaches is referred to as the *semi-quantitative* or hybrid method [27].

While the set of triples still applies, the modern approaches to risk analysis have expanded on the components of risk: In terms of risk analysis, the key components of a risk (R) related to an activity are as follows [28] (p.229): R is described as a function of events (A), consequences (C), associated uncertainties (U), and probabilities (P). U and P calculations rely on background knowledge (K) which captures the qualitative aspect of the risk, for example, low K about a risk equals more U . Model sensitivities (S) display the underlying dependencies on the variation of the assumptions and conditions. Thus, $R = f(A, C, U, P, S, K)$ allows for a comprehensive output and incorporates the most common components of risk.

In InfoSec, an ISRA method typically proposes how to derive a risk estimate, for example, FAIR (Factor Analysis for Information Risk) builds on their developed Risk Taxonomy [9]. FAIR provides definitions of each item in the taxonomy and mathematical formulae for calculating risk, the newest version [62] builds on measurement theory (proposed by Hubbard [81]) and Montecarlo simulations. While ISO/IEC 27005:2011 [15] proposes to use both the qualitative and quantitative approach, together with the Annex E dedicated to the issue. Other ISRA frameworks come with their tools for calculating probability [7, 170, 53], but in frameworks such as Risk IT[4], it is recommended that the probability calculation of an event occurring is based on historical numbers. If no such data is available, there exists other approaches to determining the probability, such as the previously mentioned Montecarlo Analysis [109, 62, 87], Interval Analysis[112] and Bayesian probability [47]. Table 2.2 shows a selection of ISRM/RA methods described with the terminology from Table 2.1 and highlights some key differences. For example, *Attack Trees* [124] and CORAS [53] are typical risk modeling tools, while ISO27005 is more of a comprehensive ISRM approach.

2.5 Research on challenges in ISRM/RA

In their review of InfoSec issues and respective research contributions Siponen and Oinas-Kukkonen [130] propose an analytical framework for studying InfoSec issues. The authors conduct a literature review and propose a classification scheme for the identified research problems. Although the study includes security management issues, it spans much wider to address more technical InfoSec issues.

Snekkenes [133] presents a taxonomy of ISRM methods using the view of key building blocks in ISRM methods. The taxonomy sorts the field into five RM activity classes which can be used to distinguish and compare ISRM methods in five categories: (i) Information

Table 2.2: Overview of a set of existing methods with categorization and descriptions

Method	Main Category	Procedure	Description
Attack Trees [124]	Model-based Risk Analysis	Qualitative or Quantitative	The Attack Tree method is constructed from a specific malicious scenario (root node), and allows the analyst to model several actions (leaf nodes) the attacker(s) can perform in order to realize the scenario. The method builds on Boolean logic with "and" or "or" gates, and Node values. The method allows for modeling of attacker capabilities and motivation. Applicable in the design phase or in analysis of major changes to existing systems.
Attack-Defense Trees [96]	Model-based Risk Analysis	Qualitative or Quantitative	The Attack-Defense tree is an extension upon the Schneier's attack trees, and allows the analyst to add defense nodes into the attack tree.
Annual and Single Loss Expectancy (ALE/SLE) [123]	Standard Risk Analysis (Can be model based)	Primarily Quantitative	ALE/SLE are prevalent quantitative methods for ISRA. The SLE is calculated using asset value (AV) times exposure factor (EF). The annual rate of occurrence (ARO). The ALE is calculated using SLE times the ARO. ALE/SLE are beneficial in the terms that the results can be used in cost/benefit analysis. Applicable in risk estimation of single and annual losses from security breaches.
Conflicting Incentives Risk Analysis (CIRA)[177]	Standard Risk Analysis	Qualitative	In CIRA, risks are modelled in terms of conflicting incentives between stakeholders and focuses on their actions and perceived outcomes of these actions. A risk is according to CIRA, when a stakeholder is in the position to trigger the action and the risk taker would be in disadvantage as in the action. The method is built on economic theories (similar to Game Theory). Applicable in scenario analysis of human interactions and incentives. Proposed as an extension of the stakeholder analysis in early phases of the SDLC.
CORAS [53]	Model-based Risk Analysis	Qualitative or Quantitative	CORAS is a seven-step method for ISRA. It uses its own Risk Modeling language based on UML. both for modeling and communication. CORAS is based on modeling threat scenarios to assets. The models are similar to trees, with an attacker/threat, vulnerabilities, risks, unwanted incidents, and impacts to asset. The risk estimation uses qualitative values, but there is room for quantification [52].
CRAMM [170]	Simplified Risk Analysis	Qualitative	The CCTA Risk Analysis and Management Method (CRAMM v.5) is a qualitative ISRA method [170]. CRAMM is sequentially built, first identifying and evaluating assets; Second, assessing threats and vulnerabilities, before combining the risk estimation and evaluation activities into a joint analysis process. Lastly, CRAMM proposes a risk management process. CRAMM is dependent on the software to utilize its full potential.
OCTAVE Allegro [46]	Standard Risk Analysis	Qualitative	OCTAVE Allegro centers on threat profiling assets. Organizational drivers provide the basis for developing risk measurement criteria. In course terms, the method is as follows: identify and profile assets within their containers, identify threats to assets, identify and mitigate risks based on threat information. The method uses threat trees as a part of the process.
FAIR [62]	Model-based Risk Analysis	Primarily Quantitative	FAIR is a method that is the predecessor of the risk taxonomy by The Open Group. The taxonomy combines four well-defined factors for each of the loss and probability calculation. Including ways to measure the different factors and to derive quantitative analysis results. The FAIR approach centers on risk assessment.
NSMROS [113]	Standard Risk Analysis	Qualitative or Quantitative	The NSMROS (Norwegian Security Authority Risk and Vulnerability Assessment) approach is a Norwegian approach for asset and object security. The goal of the method is to help organizations conduct risk and vulnerability assessments, and improve their capability to handle risk.
ISO/IEC 27005 [15]	Standard Risk Analysis	Qualitative or Quantitative	ISO/IEC 27005 is the current ISRM standard and details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. The approach is sequential with an extensive appendix, which supports the user in scoping, and asset, threat, and vulnerability assessment. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood.
NIST SP 800-30 rev.1 [37]	Standard Risk Analysis	Qualitative or Quantitative	NIST SP 800-30 is a sequential method and a threat-centric method, which suggests a threat-based approach to risk, instead of asset-based approach. SP 800-30 actively makes use of the risk framing components from NIST 800-39 [103]. It supports both types of probability estimations or hybrid. The method allows for different risk models, and the components of the estimation output are dependent on the chosen model.

2. BACKGROUND AND RELATED WORK

Discovery and Collection, (ii) Processing of collected information, (iii) Decision Making, (iv) Decision Implementation, and (v) Documentation and communication of findings and results. Snekkenes also presents a research menu for ISRM issues and research challenges which partially suggest some of the problems addressed in this thesis, in particular, related to cost/effectiveness of the ISRA method application.

Fenz et.al. [58] has compiled a list of current research challenges in ISRM challenges. The authors have reviewed multiple ISRA methods and compare them with the said list of challenges to evaluating how they perform. The Fenz et.al. study is different from this thesis in that it reviews how methods handle a predetermined set of issues, while our study identifies a set of issues and seeks to validate them with practitioners.

2.6 Comparison frameworks for ISRM/RA Approaches

In this section, we discuss the previous work conducted by others regarding ISRM/RA method comparison and how the results in this thesis differ and extend previously published work. There are several comparison studies of ISRM/RA methods in the related work: The Sandia Report [44] presents a classification scheme where ISRM methods are sorted in a 3-by-3 matrix by the level of expertise required and type of approach. The Sandia classification describes the level of skill needed to apply an ISRA approach and what type it is, either temporal, functional, or comparative.

There exist multiple comparative studies outlining ISRA approach content to aid organizations in choosing a method, for example, ENISA's high-level summary of existing methods [2] and *Methodology for evaluating usage and comparison of risk assessment and risk management items* [3]. The latter is a well-developed approach for comparing and benchmarking possible ISRM processes, together with expected inputs and outputs. The benchmark follows the classic ISRM process (Fig. 1.1), including the six main ISRM stages and fifteen defined sub-process. The ENISA method compares the reviewed frameworks to a set of items that we interpret as best practices. The former ENISA comparison [2] is a high-level comparison of methods, based on four predefined categories for ISRM and ISRA, eight in total. While similarly, Syalim et.al [142] has published a comparative analysis that applies four predefined generic steps of the ISRA process for comparison. Both these studies compare a set of ISRA methods within a predefined set of criteria. An approach that risks leaving important aspects out of the comparison. For example, both comparisons downplay the role of the asset identification and evaluation process, which, often is the foundation of the risk assessment. Bornman and Labuschagne [38] presents a very detailed framework for comparing the complete ISRM process, divided into five categories. The authors built their comparison criteria on CobiT (*Control Objectives for Information and Related Technology* (COBIT) by ISACA). This framework focuses on what the compared methods address and contains about COBIT, but not differences in how they recommend solving the task, or the distinct differences between the approaches.

Another similar study was conducted by Shamala et.al. [126] which defines a detailed information structure for ISRA methodology contents. This comparative framework was developed to evaluate ISRA methods primarily on the information structure regarding what is needed at a particular step in the assessment. Shamala et.al. focuses on how and what information to collect, our results look at how ISRA methods address particular tasks and issues.

Agrawal [17] has published a comparative study of ISRA methods, in which the author summarizes four methods using ontology. The paper compares the four ISRA methods to eight pre-defined criteria, whereas it considers if a method is primarily qualitative or quantitative, purpose, and if it is scalable. Agrawal also describes the expected input, effort, and outcome of each process step, and then discusses the pros and cons of each reviewed method.

One of the most comprehensive taxonomies of ISRA regarding reviewed methods is the

Shameli-Sendi et.al. study [127], in which the authors have reviewed 125 papers. The study provides a modern taxonomy of ISRA methods based on a set of four categories identified by the authors. The first category, *Appraisalment*, is defined as the type of input and output of the risk calculation, such as if it is qualitative, quantitative, or a combination of both (hybrid). The second category addresses the ISRA method's *Perspective*, which is either business, asset, or service-driven. An additional category, *Threat-driven* [37], could also have been considered for the perspective category. The third category, *Resource valuation*, which primarily considers how the ISRA method suggests evaluating valuables: either asset, service, or business process, and if it considers functional dependencies between them. Whereas compromising one asset may inflict consequences on another, and such on. The fourth category is *Risk Measurement* in which the taxonomy classifies ISRA methods regarding how they consider impact propagation, meaning if the method advises considering an impact only to the asset itself (non-propagated) or if it considers dependency between assets and other resources. The Shameli-Sendi et.al. taxonomy considers how an ISRA method classifies within the predefined criteria identified by the authors. Typical for all of the existing comparison methods is that they predetermine a fixed set of criteria which is used to study a set of ISRA framework. They all have their merits, but the reviewed comparison methods are equivalent to a top-down comparison. What if the most important differences in application lie outside of the defined set of criteria?

2.7 Empirical comparisons of ISRM/RA

In his book "*The Failure of Risk Management*", Hubbard [80] challenges several perceptions regarding today general RM practices, most of which also apply for ISRA. In particular, how do we know what works in risk management? Snekkenes [133] also touches on several related topics, however, empirical research on ISRA is required to answer address this problem, but we found that this area remains largely unexplored for ISRA. The study by Kotulic and Clark [97] proposes a possible answer to this situation and highlights that there are very few empirical studies of within information security. In their study, the authors present a conceptual Security Risk Management model which they attempted to validate but found that it is hard to obtain results. This was partly explained due to InfoSec being one of the most intrusive types of research. Further, they explain 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 explanations 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. These challenges are still obstacles for conducting empirical InfoSec research, but since the Kotulic and Clark study, several researchers have found ways around these issues for gathering empirical data: for example, Bulgurcu et.al. [39] investigated information security policy compliance and awareness using motivational theory and beliefs. They collected their data sample using anonymous online surveys by employing a third party market research company. A study on a similar subject conducted by Johnston and Warkentin [86], investigates fear appeal theories and models on InfoSec behaviors. The authors designed the study as a laboratory experiment using university students as their subjects. There are also several empirical economic types of research on information security, such as an analysis of the economic cost of publicly announced information security incidents [43], where the authors gathered and analyzed data from the stock market. Spears and Barki [139] conducted a study on user participation in ISRA, and found that it benefited the quality to include users. In addition to empirical studies of security culture [92, 120]. Sufficient to say, it is possible to overcome the challenges to conducting empirical research in InfoSec. However, regarding research on ISRM, we found the current literature to be lacking.

2.8 Cyber Security Risk Modeling

This section addresses related work in three parts on InfoSec risks: (i) reviews work on typical risk modeling tools, (ii) Discusses risk quantification, and (iii) Discusses limitations of risk forecasting for InfoSec.

2.8.1 A review of risk models

Several of the mentioned methods model risks visually, typical examples are Event-tree and Fault-tree analysis, where risk is modeled as a set of conditional events. These approaches are not typical for InfoSec. However, Schneier adapted the Fault-tree analysis mindset and created *Attack Trees* [124]. These are basic graphical and mathematical tree constructs that consider possible vulnerabilities and attack options for an adversary, where each node uses Boolean logic and is prescribed a subjective possibility: possible or impossible. However, the possibility values can be exchanged with probability. The Attack tree for InfoSec opened a research venue for modeling InfoSec risk whereas several research papers build on and improve the approach. For example, Mauw and Oostdijk [108] provide a formal interpretation and semantics to the attack tree, while Kordy et.al. [96] expands the concept into an Attack-Defense tree by adding defense nodes into to the model. The defense trees have also been explored as defense graphs with architectural models [136], in which it combines expected loss and Bayesian statistics. Further, the attack tree model of an InfoSec risk has been researched in a variety of areas, such as Smart grids [49], SCADA Systems [41], Threat modeling [121], and Attacker profiling [101]. The application of the attack tree are many, and it has a high utility, such as the ability to model complex systems and events into sequential steps that promote understanding and holistic thinking. The models allow the analyst to consider several venues of attack and provide countermeasures, in addition to being adaptable for adding new venues of attacks as they are discovered. However, there are also some limitations: ICT systems continue to grow in both size and complexity which also introduces new vulnerabilities and larger attack surface. The attack tree addresses only one initiating event at a time, which means that the amount of discovered vulnerabilities and threats can create a lot of risk models that needs to be created and maintained. Since each attack tree is built on an initiating event, a new model must be constructed for each identified initiate event. This development means a lot of risk models to maintain, also, comes the increased complexity of the systems that must be mirrored by the models. Model completeness is a challenge, as it is easy to overlook possible attack pathways. There are also limitations in considering an attack a success or a failure, for example, what if an attack is a partial success? Deriving probabilities for each node in the attack tree is also a challenge, whereas, the lack of quantitative forecasting data is a challenge for such specific events [68, 26, 29]. The number of nodes in the tree will also reflect the calculations needed to reach the probability of the event, and an increase in calculations will increase the room for error and should decrease the confidence in the results.

Further, there exist several tools for modeling risk, for example, the CORAS method is a UML-based risk modeling language [53, 52]. CORAS centers on modeling threat actors, vulnerabilities, assets, and controls which resemble an attack tree. Figure 2.1 illustrates a CORAS risk model of an access control violation. As the illustration shows, the CORAS legend makes the model quite comprehensible. The CORAS approach builds on the same principles as the ISO27005 standard [15] proposes but substantiates the risk modeling process. The risk estimation uses qualitative values, but there is the possibility for quantification.

Another example of a distinct method which avoids the probability problem is the Conflicting Incentives Risk Analysis (CIRA) [117], which represents a different approach to risk assessments. CIRA frames risk in terms of conflicting incentives between stakeholders, focusing on the stakeholders, their actions and perceived outcomes of these actions. The risk owner and the strategy owner are the two classes of stakeholders in CIRA. The perspective

2. BACKGROUND AND RELATED WORK

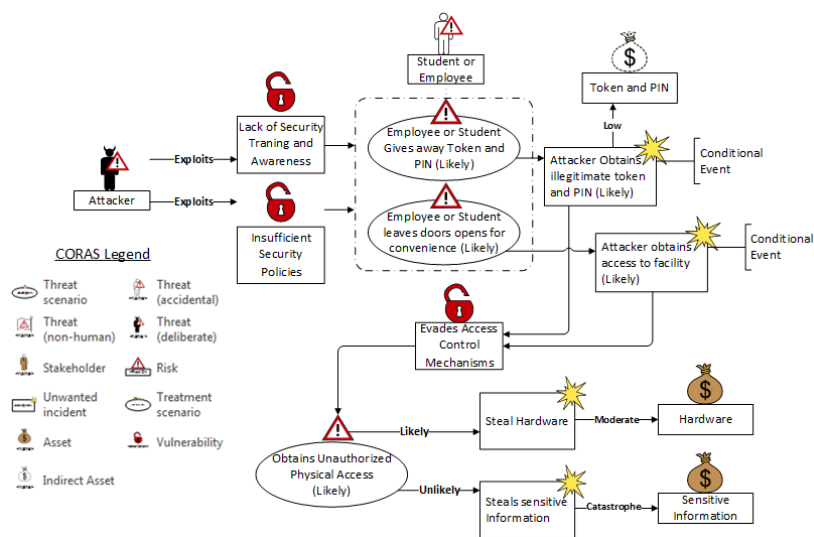


Figure 2.1: A CORAS model of an access control risk [149].

for CIRA analysis is that of the risk owner. A strategy owner is capable of triggering an action to increase his perceived benefit. CIRA applies terms from economics where the corresponding stakeholder defines "utility" as the perceived take advantage of triggering an action. According to the method, utility factors are weighted by how much the stakeholder values it while the initial value represents the status of the utility factor. Risk treatments in CIRA are controls that disincentivize unwanted behavior or strengthens the incentives for desirable outcomes. Thus, the risk model is based on incentive structures and perceived disincentives as seen by the stakeholders. In this case, the risk manager must adjust misaligned incentives, rather than, for example, managing technical vulnerabilities. Therefore, CIRA has some limitations when it comes to InfoSec since it requires a thorough understanding of the adversary to model the incentives, often, we do not know the adversary at all since he is attacking from the other side of the planet.

Another approach to modeling InfoSec risk is relational models, Sommestad et.al [137] proposes a probabilistic relational model for security risk analysis for architecture metamodels. The authors suggest classes, attributes, and class relationships for their model using UML. An advantage of this model is that it visualizes probabilistic dependencies between the attributes and that the models allow for a comprehensive modeling of the target system. Some disadvantages of this approach is that the models can become quite complex and hard to comprehend, inherent is also that will be hard to communicate to stakeholders. The proposed model depends on expected loss (ALE/SLE) for their risk calculation. The probabilistic relational model [137] provides the framework for the Cyber Security Modeling Language (CySeMoL) [135] which is a tool for modeling and assessing the vulnerability of enterprise system architectures.

The reviewed literature for risk modeling only represent a small piece of all the available tools and methods available to a risk practitioner [127]. We find the risk modeling domain quite mature, but it seems that the risk estimations of probability and consequence that represent the biggest problem.

2.8.2 Risk Quantification approaches

From the discussion in the previous section, we see that estimations are at the center of the debate regarding ISRA and that different risk assessment approaches often come with distinct estimation methodologies. Often, a method is either defined as quantitative or qualitative, which all the associated difficulties. The Single and Annual Loss Expectancy (SLE/ALE) represent one of the most applied areas of statistics (quantitative) in ISRA [71] (P.87). In ALE, the risk is described as the probability of a loss occurring [123]. Another approach for quantifying and measuring the benefits of an InfoSec investment is the *Return on Security Investment (ROSI)* models [138]. Measuring and managing InfoSec risks are difficult because a lot of the time the organization is implementing measures to mitigate a risk for which they do not know is going to happen or not, and it can prove difficult to verify if such as a preventive control is effective. Sonnenreich et.al. [138] discusses techniques that can be used to measure security within an organization and financial justification of security investments. The ROSI approach is a modification of a traditional ROI (return on investment) calculation, where expected returns are substituted with (Risk Exposure x %Risk Mitigated). However, both ALE and ROSI are dependent on historical data, in addition, Aven [29] argues that risk must be considered as more than expected loss. Aven's argument expected values can misguide decision-makers, mainly because we *seldom have a huge number of similar activities with known variations as the law of large number presumes* [29] (Appendix A). Consider the implications of this argument for an attack tree with multiple nodes: In which each node is a barrier the attacker must scale, the system being complex with multiple attack vectors and vulnerabilities, and the attacker's capabilities and capacities varying. We can also view the information system as organic, in which it develops on a day-to-day basis, with new patches, software, hardware, and infrastructure. As one attack vector may have different variables from one day to the next, Aven's argument holds true for InfoSec as well and defines the core of why it is hard to quantify InfoSec risk. Rather, Aven argues that statistics should be used as a risk index or metric in situations where it can be informative.

The Factor Analysis for Information Security (FAIR) [62] has taken steps towards addressing the issue of data availability. FAIR provides a taxonomy of InfoSec risk, where every aspect is probabilistically defined. The method addresses the data availability problem by applying measuring concepts based on human expert estimation supplemented with calibration techniques for obtaining distributions through Montecarlo simulations. The Montecarlo approach is further substantiated for cyber security by Hubbard and Seiersen [82]. Running Montecarlo simulations to obtain a probability distribution based on few measurements or expert predictions has both advantages and drawbacks. The main advantage is that it removes some data dependencies in the estimation. The drawback is that the risk model's sensitivity is likely to be presented as more stable than it is since the dependency on the Law of large numbers is removed: the model is quantifying expert estimations that may be off target, although the authors argue that calibration vastly increase the precision. While risk quantification certainly has merits, another issue is that all variables do not need to be quantified to provide a reasonable input to the decision-maker since the goal is to optimize decision-making, not to put numbers on every variable. However, the Hubbard and Seiersen-approach to cyber security is at the time of this writing a new approach (published 2016) and more empirical research on the method is required to determine the utility.

2.8.2.1 InfoSec risk classification

With his book "The Black Swan" [144], Taleb established himself as an authority among the unpredictable in risk management and analyzes the limits for forecasting. With the Black Swan theory, Taleb describes rare, extreme and unpredictable events of enormous consequence. These events, known as Black Swans, are so rare that they are impossible to predict and go beyond the realm of reasonable expectations. A Black Swan has three

2. BACKGROUND AND RELATED WORK

properties [144]: Firstly, it is an outlier, falling outside of the realm of regular expectations because nothing in the past can convincingly point to its possibility. Secondly, it carries an extreme impact. Lastly, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, rendering it explainable and predictable. A Black Swan is fat-tailed distribution and exposure to them can be both positive and negative. Taleb describes innovation as an area that has a very little downside and a large upside (convex), small investment and large profit. While describing finance as having negative Black Swan exposure, where large losses are possible in a short period e.g. financial crisis 2008 (concave).

Before labeling every InfoSec risk a Black Swan and concluding that we can not predict anything, consider the antithesis, Hubbard and Seiersen [82], which argues that we can measure everything in Cyber risk. However, the world is seldom black or white, and there are there are levels of predictability for each risk. Taleb recognized this issue and proposed the Four Quadrant risk classification system [143], which consists of two types of *randomness* and *decisions* to classify risk according predictability. The former is described in the core concepts of Black Swans as *Mediocristan* and *Extremistan* randomness.

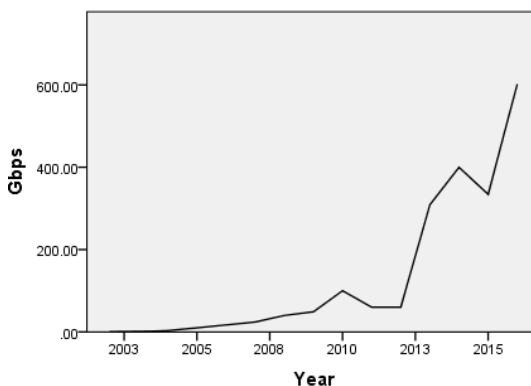


Figure 2.2: The development of bandwidth consumption (Gbps) of DDoS-attacks during the last 15 years. *Data source: Arbor Networks and media reports*

In *Mediocristan* (First and Second Quadrant) risks are predictable, and the Gaussian bell curve applies. Examples of *Mediocristan* is found in human height, weight and age probability distributions, where the average member is average, or "mediocre," and no single outcome can dramatically change the mean. *Mediocristan* is non-scalable and subject to only mild randomness. We can accurately predict events in *Mediocristan* based on historical data and the Gaussian Bell curve with little amount of uncertainty. In *Extremistan* randomness (Third and Fourth Quadrant), small probabilities and extreme events rule. Estimation of small probabilities is very error-prone, since the sample set is so small and small changes in the calculations have major impacts on the results, e.g. $P=0.1\%$ and $P=0.01\%$ of an event occurring once a year, are both very unlikely risks, but very different and sensitive to new information. In *Extremistan*, events scale and are subject to *fat-tails* and can appear as power law or Pareto distributions. Further, *Extremistan* is often a product of the modern society and interconnectivity, which in turn makes it more informational than physical. *Extremistan* is Black Swan domain, and *fat tailed*, examples of improbable ICT events are the consequences of the Morris worm [114], the Malware development trend Fig.2.3, or the rapid increase in DDoS capacity Fig. 2.2.

There two types of Payoff in Taleb's four quadrants: (1) Simple Payoffs and (2) Complex Payoffs. In the former, decisions are binary-type, e.g. either true or false. This is where

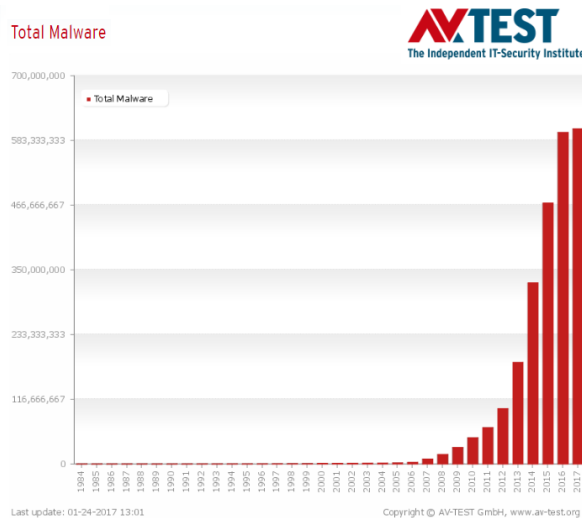


Figure 2.3: Malware development from 1984-2017. Source: AVTest - The Independent IT-Security Institute (<https://www.av-test.org>). Reprinted with permission

mainly probabilities play, such as in games. For the latter, decisions are more complex, where the decision maker must also consider the impact or a function of the impact. Type 1 is thin-tailed and non-scalable, while type 2 decisions can be fat-tailed.

The Four Quadrants links risk to decision theory, whereas the purpose is to classify the two distinct types of decisions (Simple and Complex) and classes of randomness (Mediocristan and Extremistan) for each risk, see Figure 2.4. Briefly explained, the First Quadrant has Mediocristan randomness and low exposure to extreme events. The payoffs are simple and statistical models works. The Second Quadrant is exposed to Mediocristan randomness with high exposure to extreme events. The Third Quadrant is exposed to Extremistan randomness and low exposure to extreme events. The Fourth Quadrant is "the area in which both the magnitude of forecast errors is large, and the sensitivity to those errors is consequential"[143].



	1 Simple Payoffs	2 Complex Payoffs
A Mediocristan 	First Quadrant Extremely Safe	Second Quadrant (Sort of) Safe
B Extremistan 	Third Quadrant Safe	Fourth Quadrant Black Swan Domain

Figure 2.4: Taleb’s four quadrants for Risk Classification. Based on Taleb[143]

2.8.2.2 Black Swans in InfoSec

Taleb's concepts are not without controversy; in his book review of *The Black Swan* from 2008, Prof. Denis Lindley criticizes the concepts and argues that our existing methods are more than good enough for estimating risk. While Hubbard [80] dedicates Chapter eight of his book discussing and criticizing Taleb's concepts. The Black Swan concept has been extensively treated for general risk analysis in Aven's articles [31, 30]. Aven [31] discusses where the main contribution of these concepts to risk analysis lie and their shortcomings. Among the adoptions of Taleb's four Quadrants, Zeisberger and Munro [172] has addressed several aspects which they describe as shortcomings of the original four quadrants. For explicitly information security risk, the Black Swan concept has been treated by Hole and Netland [79], who analyses large-impact and rare events in ICT. Where the authors provide a basic discussion of what black and gray swans are in information systems and discuss events that may qualify as Swans. They define cascading risks and single points of failure as sources for swans, and worms, viruses, and other malware are sources for cascading risks. Hole and Netland also establish evidence supporting that information system are susceptible to rare and surprising events. Additionally, Hole [78] addresses how to manage hidden risks, and how to recover quickly from Black Swan ICT incidents. In his compendium "E-bombs and E-grenades" (P.28-37)[26], Audestad provides the literature that comes closest to discussing the issues of this article from an information security perspective. Audestad does not use the term Black Swans, but he describes extreme events, limitations of statistics, and provides the mathematics to support his views. However, the predictability, properties, and limiting factors for forecasting of individual InfoSec risks are largely neglected in the ISRA research.

2.9 Summary of Related work

On the research problems in ISRM, the gap was that we did not find a comprehensive structuring of research problems with a corresponding validation study. The related work contains several approaches to comparing method content. While several of the comparison frameworks are comprehensive, these are primarily studies of properties and content based on a predefined set of criteria. None of which address how to compare full ISRA processes and content beyond these criteria. Thus, the gap in the research literature lies in the lack of a bottom-up approach to compare ISRM/RA methods. Neither did our literature review reveal any previous empirical research on practical ISRA application for studying cause-effects. For risk modeling, we found that there exist several approaches to both modeling and quantifying risk, many of which are rooted in the Fault or Event tree methodology. Further, the literature review revealed several different opinions on risk quantification and the usefulness of the expected value. However, few have explored the limitations of the quantitative approaches beyond the Black Swan [79, 78] and none had explored the issue of predictability for individual InfoSec risks. We identified a gap regarding the factors that limits prediction, which are properties the analyst should understand before embarking on risk quantification. In addition, ISRM methods claim to be mainly quantitative [36, 62] or qualitative [46], but the quantitative versus qualitative risk situation is not strictly either-or. There is utility in both approaches and degrees of subjectivity in any risk assessment, and the intersection of these two approaches remains largely unexplored.

Research Method

This Chapter summarizes and explains the basis for scientific research and method. Further, it describes the applied method for each article in this thesis in the frame of Design Science Research. First, we summarize, discuss, and justifies the overall choice of method. Second, we describe the methods applied to address each research question and discuss knowledge contributions in the frame of Design Science Research.

3.1 Summary of Considered Research Methods

Scientific research is "*a systematic process of collecting, analyzing, and interpreting information (data) to increase our understanding of a phenomenon about which we are interested or concerned*" [100]. There are many requirements for something to be called scientific research, one of the key issues are ensuring consistency in the method choice and description. The method description enables reproducibility of scientific results through duplication of experiments by independent scientists, which is one of the cornerstones of scientific research. Further, the scientific method allows for several scientists to produce evidence for or against a hypothesis and to accept or reject the same hypotheses when considering the aggregated evidence. The key steps in the scientific method are to define a problem, review related work, form a research hypothesis or research questions, and choose a suitable method for hypothesis testing. The primary goal when selecting a research method is to find a feasible and sensible method for collecting data that can be analyzed to answer each research question [100]. Thus, the scientific methods build on systematic observations, measurements, and experiments for testing and modification of hypotheses. These activities are guided by research methodologies to comply with requirements of scientific research. Broadly, there are two high-level approaches to research, *deductive* and *inductive*. Saunders et.al. [122] explains that deductive research is to develop a theory and/or a hypothesis and develop a research strategy to test the hypothesis. The deductive strategy typically requires rigorous and repeatable experimentation to reject or accept the hypothesis. Further, Saunders et.al. [122] describes the *inductive* approach as when the researcher collects data and as a result of the data analysis develops a theory. Thus, the inductive method is typically applied to conduct research on real-world and complex problems.

Further, there are two main approaches to gathering research data, being *Quantitative* and *Qualitative*. The *Quantitative research* approach is to base the conclusions on amounts, or quantities, of data [100]. Quantitative research typically involves statistical analysis of data samples in order to test a hypothesis. **Surveys** is a quantitative approach [100] for gathering data that can easily be used for statistics. E.g. online surveys allow for easy access to the survey itself, and this approach can yield large quantities of relevant data. *Mathematical modeling* is a quantitative method, which i.e. can be used to represent complex mathematical and statistical relationships[122]. Another example of quantitative research on a complex system using mathematical modeling is the weather forecast. In which the researchers gather large amounts of data from multiple measurement points to predict the developments in weather trends. One can also use *Statistical analysis* to collect and analyze large quantum of data, typically no less than a sample size of thirty [122].

The *Qualitative research* approach is used for looking at characteristics, or qualities [100] of data. The qualitative approach is often employed in social sciences, with the aim of un-

3. RESEARCH METHOD

Research Phase	1. Problem Identification	2. Problem Id. & Validation	3. Develop, Define Req. and Design Artifact	4. Demonstrate, Validate, and Develop Artifact	5. Artifacts
Applied Method	Literature Survey and Analytical Comparison	Questionnaire and Statistical analysis	Literature survey, qualitative analysis, and modeling	Case study, Feasibility Study, and Qualitative analysis	Knowledge, Construct, Model, & Method
RQ Publication	RQ I & II Article I & II	RQ III Article III & IV	RQ IV Article V	RQ V & VI Article VI-VIII	

Figure 3.1: Research phases together with a summary of applied methods, RQs, and published articles

derstanding phenomena such as human behavior and the underlying reasons.

Scientific *Modelling* is the process of generating a model to help solve a problem. The models are mainly used to model either phenomena, data and theory [63]. As this method investigates a particular phenomenon, it is mostly a qualitative approach. A *Case study* is according to Flyvbjerg [59]: *...an intensive analysis of an individual unit (e.g., a person, group, or event) stressing developmental factors in relation to context*. The strengths of case studies is that they can explore a concept in depth and it has a high conceptual validity.

Scientific *interviews* is a qualitative approach to solving a problem [100], for example conducting face-to-face interviews with questions outlined in advance. *Grounded theory* look for patterns in collected situational data, *Instead of starting with a theory begins with an area of study and what is relevant to that area is allowed to emerge* [66]. *Action research* is a form of applied research where the researcher attempts to find a solution to a local problem, e.g. by participating directly in a project [100]. *Literature review* is an empirical survey of existing literature within the field of research [100].

3.2 Applied Research Method

According to March et. al.[107], much of the research conducted within information systems are either behavioral science or design science. Hevner[75] further explains what sets these two apart; *A behavioral science paradigm seeks to develop and verify theories that explain and predict human or organizational behavior, and the design-science paradigm seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts*. The *Design science* research method is specific for conducting research in information systems and consists of a set of analytical techniques[98], and is fundamentally a problem-solving paradigm[75]. The research presented in this Thesis is of risk assessment in information systems, which overlaps into the technical, organizational, and human domain. Thus, the overall research project in this Thesis is an adaptation of the Design Science Research (DSR) paradigm. DSR addresses unsolved research problems experienced by stakeholders within a particular practice and solves them in unique or innovative ways [74] (P. 15). The result of DSR should, according to Hevner et.al. [75], *"be a purposeful IT artifact created to address an important organizational problem. It must be described effectively, enabling its implementation and application in an appropriate domain."* The artifact should be in the form of constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems).

The first step of the DSR process is to define the problem, and, further, to determine the requirements, design, and develop an artifact to address the problem. Followed by a demonstration, evaluation, and development of the artifact.

Since this Thesis deals with complex and real world problems, the primary high-level method is inductive research. DSR is the overarching framework that describes this research, however, for each of the RQs we have applied a set of scientific methods to gather data, analyze, and provide an answer. This thesis contains research that categorizes within

both qualitative and quantitative research, primarily the former. Fig. 3.1 summarizes the sub-projects in this Thesis. The first phase is the problem identification phase, where our goal was to obtain a comprehensive insight into the theoretical domain. Specifically, it investigates known challenges for ISRM/RA and their implications for decision-making. The primary research methods in this phase were the literature review and qualitative analytical comparison. The second phase of the research was the Problem Identification & Validation-phase, which investigates the practitioners view on ISRM/RA issues. Having established the necessary understanding of the problem domain, in the third phase, we develop the artifact which focuses on defining requirements and designing an ISRA method comparison model from the bottom up. The fourth phase demonstrates the utility of the artifact by developing it and applying it in two different and novel settings. The output of each phase is the input for the next phase.

The following sections provide a short description of each sub-problem together with a method description.

Defining the problems (RQ I & II):

This study applied for a qualitative literature review to define the known problems within the ISRA research field. In which, we gathered data and synthesized a taxonomy of known research problems, and categorized them within the ISO/IEC 27000 [11] vocabulary. The primary purpose of our taxonomy was to categorize and present findings at different stages in the ISRM areas and activities. In order to obtain a more comprehensive theoretical understanding of the problem domain, we also identified a need to compare the InfoSec with other management frameworks to pinpoint additional under-prioritized areas or problems in the ISRA domain. The results from these studies provided the background for the next step in the research project.

Validating and Expanding the problems (RQ III):

Since the nature of studying RQ I & II were limited to findings from the academic literature and was scarce regarding the current ISRA industry practices, this study aimed to research the risk practitioners point-of-view. In particular, if they agree that our initial findings were relevant, representative, and complete. There were primarily two available approaches for this inquiry, either interviews or questionnaires. The former would limit us to local experts, produce a smaller sample size, and require more resources. Thus, we chose to use online survey and statistical analysis. We designed the questionnaire based on the findings from answering RQ I & II, and the questionnaire had category, ordinal, and continuous type questions. The main bulk of questions in the survey were designed using several mandatory scales- and ranking questions. The questionnaire also included several non-mandatory fields for commenting on previous questions or just for sharing knowledge about a subject. The participants were recruited from expert and topic-specific ISRA forums.

Developing artifact (RQ IV):

One of the primary findings from the initial research was that there are several ISRA frameworks and methods (see Shameli-Sendi et.al. [127]). However, there was no empirical research on method application and differences in results. Reviewing this problem, we found that the research field for ISRA method comparison was quite saturated (e.g. [2, 38, 142, 126, 44, 127, 17]). The existing approaches yielded differences within a predetermined set of criteria, but overlook the differences that are not present in the criteria, which are relevant for cause-effect studies of method application. In other words, the existing comparison frameworks were equivalent to the top-down approach and made them less suited for comprehensively mapping ISRA items not present in the criteria. Our research revealed that there was no comprehensive bottom-up comparison of the frameworks, which was necessary in order to compare methods on completeness and reveal focus areas. This scheme makes them less suited for analyzing cause-effect relationships between method and results, since causes not present in the criteria may be neglected.

The CURF bottom-up approach solves this problem by mapping ISRA method content and using it as comparison criteria. For each added method reviewed in CURF, we iden-

tify which tasks the approach covers and combine all the tasks covered by all surveyed methods into a combined set. The evaluation of the ISRA method consists of investigating to what extent the said method covers all undertakings present in the already created super-set. The super-set should provide the practitioner with insight into which aspects each method cover, together with an overview of where to seek knowledge in the literature to solve other specific issues or for comparison purposes.

We both designed the artifact, CURF, and continuously developed and demonstrate it through classification of ISRA methods within the framework and improving the model. We evaluate the model by applying the comparison scheme on the existing methods by adding all standalone tasks and deriving new knowledge.

RQ V, Demonstration, Validation, and Development:

Numerous ISRA methods have been developed throughout the years [127], this development has created a situation in which there are many InfoSec risk assessment (ISRA) approaches to choose from, but scarce information on how to choose and if the choice of method matter for the result. This RQ explores the latter where we have applied three different ISRA methods on various case studies and produced risk assessment results. For the case studies, we considered three main types of differences between ISRA methods:

1. *Empirical comparison through practice:* We gathered experience data from the risk assessment teams using *scientific interviews* and *online questionnaires*, both of which followed the same format and had identical questions. We analyzed the data both qualitatively and statistically depending on the data type.
2. *Theoretical comparison of frameworks:* We applied and expanded the results from answering RQ IV, CURF, in order to theoretically compare the three ISRA methods.
3. *Comparison of risk assessment results:* This was solved by applying the CURF idea in a novel manner, in which we *qualitatively analyzed* the meta-data of each risk assessment result to derive the differences from applying each method. Further, this analysis was extended to a *cause and effect study* between the theoretical CURF results and the CURF risk assessment results.

Thus, we demonstrated the utility of CURF by developing it to compare ISRA results and analyze cause and effect between method choice and process output. In this setting, CURF was a novel solution to a novel problem.

RQ VI, Demonstration, Validation, and Development:

The quantitative versus qualitative risk situation is not strictly either-or since there are degrees of subjectivity and human-made assumptions in any risk assessment and the intersection of these two approaches remains largely unexplored. In answering what the limitations and requirements are for a hybrid risk assessment model, for part one of this study [162], we conducted a *feasibility study* for statistical risk models in ISRA. Our approach was grounded in the Black Swan Theory [144, 143], described in Chapter 2. We adopted The Four Quadrants risk classification system [143] to address the feasibility of using statistical methods to predict information risks. Further, we gathered data on various InfoSec risks, analyzed them, classified them within the Four Quadrants, and discussed factors which limit risk prediction.

For part two of this study [163], we further developed the initial risk model of the DDoS-attack (Distributed Denial of Service) from part one using the *case study* methodology. In building the case study, we used technical data from a local institution and anonymized as required. Akamai Networks were kind enough to supply us with statistical data on DDoS attack magnitude and duration distributions [19] for our quantitative risk models. We applied the CURF results to build the qualitative part of the model by constructing a state-of-the-art risk model. We combined the qualitative and quantitative models using an *Event Tree*, which is a logical modeling technique for exploring conditional probabilities of events and outcomes [33].

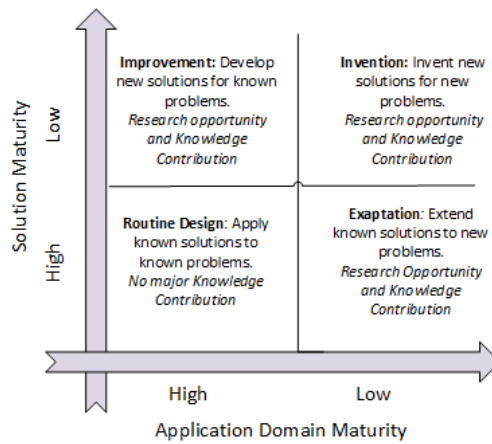


Figure 3.2: DSR Knowledge Contribution Framework based on Gregory & Hevner [68]

3.3 DSR Knowledge Contributions

Hevner [74] (P.15) writes that *the key differentiator between professional design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies and the communication of the contribution to the stakeholder communities*. One of the keys to DSR is to develop an artifact, demonstrate, and communicate its utility. For this purpose, recent work on DSR methodology has provided the community with the DSR Knowledge contribution framework [67], Fig. 3.2, which defines the DSR contributions utility within four quadrants. The quadrants are described with *Solution maturity* (SoM) on the Y-axis and *Application Domain Maturity* (ADM) on the X-axis, both scored subjectively using "high" and "low." A high ADM and SoM constitutes a known solution to a known problem, referred to as the routine design. A high SoM and low ADM is an Exaptation, where a known solution is applied to a new problem. A low score on both is classified as an invention, as it is a new solution for a new problem. Our contributions are discussed and presented within the frames of the DSR quadrants.

Summary of Papers

This Chapter summarizes the published research papers included in this thesis, eight in total. We present a short abstract together with the key findings of each paper. Figure 4.1 illustrates the relationship between the papers.

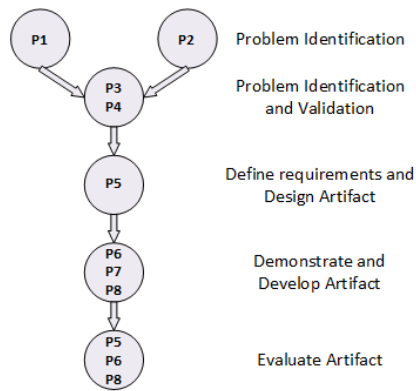


Figure 4.1: Relationship between Research Papers.

4.1 A Taxonomy of Challenges in Information Security Risk Management [164]

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

The Taxonomy of challenges builds on the ISO/IEC 27005:2011 Risk management process description using the vocabulary from ISO/IEC 27000:2009 [10], illustrated in Figure 4.2, and is a categorization of identified research issues in academic literature. The taxonomy is presented top-down model using levels and is illustrated in Figure 4.2, the following is a description of each level with a summary of key findings:

- **Level 1, The Information Security Category:** This category contains high-level findings in information security that affect ISRM, these findings did not fit sensibly into the taxonomy because of being a more wide spread issue. The key findings on this

4. SUMMARY OF PAPERS

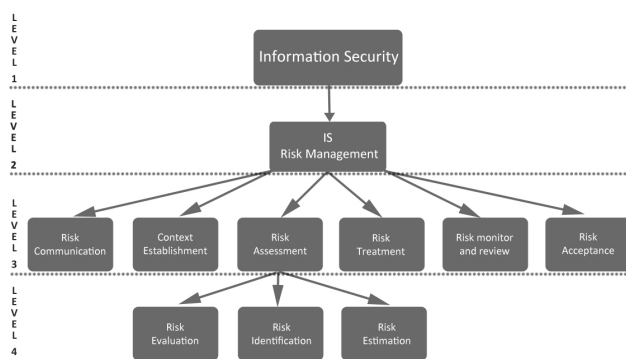


Figure 4.2: Classification scheme in the Taxonomy of Challenges for ISRM

overarching level was that ISRM was biased towards having a technical scope by prioritizing to evaluate technological aspects, which made it a challenge to detect and treat risks within human performance. Two additional key findings, first, was that there was that the majority of the published InfoSec literature was based on opinion, anecdotal evidence, or experience, which are all weak evidence. This lead to a problem we called "Lack of Empirical Research and Good Data". Second, was that there was little or no independent testing of InfoSec measures and controls, which was a challenge we called "Lack of Validation and Testing". In addition to these findings, the paper also substantiates challenges on "Common InfoSec Language" and "Conflicting Incentives and Human Factors".

- Level 2, The IS Risk Management Category:** This category contains general findings in ISRM/RM that did not fit into any of the RM activities on level three of the model. This level repeats two of the findings from Level 1, "Biased Scope and Misconceptions" and "Lack of Empirical Research and Good Data," and adds specific findings appropriate to Level 2 in the Taxonomy. Regarding the former, our results concern organizational understanding for ISRM, risk quantification in an organizational context, and misconceptions regarding ISRM programs. Regarding Empirical research, we discuss ISRM program validation, threat forecasting, and statistical data. "Existing RM methods" represents the last category at this level and critiques existing qualitative risk assessment approaches and practices.
- Level 3, The Different Risk Management Categories:** This level contains a classification for all of the identified ISRM activities (see figure 4.2). The findings from the survey are categorized within the activity that they are performed. Our key findings from this level were "Organizational Disconnect" which is when the security program does not take day-to-day operations and value production into consideration and the "Risk Vocabulary" finding which concerns the non-standardized language in InfoSec risk communication. Level 3 in the Taxonomy also discusses treatment strategies, decision making, and validation and measurements.
- Level 4, The Risk Assessment Category:** This level contains the findings for the risk assessment category, sorted in the two risk analysis activities "Risk Identification" and "Risk Estimation," and "Risk Evaluation." These findings on Level 4 are the most extensive and discuss the following challenges: Asset evaluation issues, qualitative and quantitative risk estimation, risk perception and framing, and missing significant risks, such as cascading risks, common mode failure, and Black Swans.

4.2 A COMPARISON BETWEEN BUSINESS PROCESS MANAGEMENT AND INFORMATION SECURITY MANAGEMENT [165]

Domains BPM	1.Organization and Strategy	2.Stakeholder Relationships	3.Policy and Rules	4.Information and Knowledge	5.Human Capital	6.Enabling Technology	7.Support Infrastructure
ISM Domains							
1.Information Security Policy	X 0		X 0	X 0	X		
2.Organization and IS	X 0	0	X 0	0	X	X	X
3.Human Resources Security	X		X 0	X 0	X 0	X	
4.Asset Management	X		X 0	X 0	X	X 0	X 0
5.Access Control			X 0	X 0	X 0	X 0	X
6.Cryptography			X 0	0	X	X 0	X
7.Physical and Environment Security			X 0	0	X	X 0	X 0
8.Operations security	X		X 0	X 0	X	X	X
9.Communications sec			X 0	X 0	X	X	X 0
10.System acquis, develop and mainte			X 0	X 0	X	X 0	X
11.Supplier relations		X (0)	X 0	X 0	X 0	X	X
12.IS incident man	X		X 0	X 0	X	X 0	X
13.IS aspect of BCM	X		X 0	X 0	X	X 0	X
14.Compliance			X 0	0	X	X	

Figure 4.3: Summary of BPM-ISM and ISM-BPM comparison. Legend: - "X" marks how the ISM domains are covered and can be implemented in the BPM domains. "0" marks which ISM domains support support BPM domains and where.

4.2 A Comparison between Business Process Management and Information Security Management [165]

Information Security Standards such as NIST SP 800-39 and ISO/IEC 27005:2011 are turning their scope towards business process security. And rightly so, as introducing an information security control into a business-processing environment is likely to affect business process flow, while redesigning a business process will most certainly have security implications. Hence, in this paper, we investigate the similarities and differences between Business Process Management (BPM) and Information Security Management (ISM) and explore the obstacles and opportunities for integrating the two concepts. We compare three levels of abstraction common for both approaches; top-level implementation strategies, organizational risk views & associated tasks and domains. With some minor differences, the comparisons show that there is a high similarity in the implementation strategies, organizational views, and tasks of both methods. The domain comparison indicates that ISM maps to the BPM domains; however, some of the BPM domains have only limited support in ISM. By comparing we found that there was a substantial similarity between the BPM Methodology framework and the ISRM standard NIST SP 800-39, as both approaches use similar organizational views, only applying different names. We also found that the tasks and goals of each level are similar, with some key differences: the tier/level 1 ISRM approach does not include an activity for managing enterprise processes, and BPM does not contain risk-based investment optimization and trust issues. When comparing BPM and ISM domains, we found that BPM can support the ISM tasks, but that BPM does not include the concept of internal or external attackers. Further, we found that ISO/IEC 27001/2 standards emphasized, but not controlled that the IS policy was aligned with business requirements, the overlap is illustrated in Table 4.3. We also found a significant gap between how much emphasis ISM and BPM put on stakeholders. Where BPM have fully adopted

the principles of stakeholder management and recognized its importance, there is no real approach taken in ISM to address stakeholders. We also found that the need for securing knowledge is possibly underestimated in ISM.

4.3 An Initial Insight Into InfoSec Risk Management Practices [157]

This paper is part one of two on the practitioners view on InfoSec issues (P3 & P4), where the first paper address ISRM and the second address ISRA. The two papers contain different results from from the same study.

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.

The study documents several issues concerning security measurements and returns on investment for the ISRM program, together with other relevant paths for future studies. The main conclusions of this work were that 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. Regarding ISRM 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, Table 4.1. Whereas our respondents from bigger companies did not think the ISRM program to be contributing much to business-related areas, such as productivity. Our results identified compliance with laws and regulations as the primary driver for doing ISRM work. From the practitioner's 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.

Table 4.1: Perceived contributions of the ISRM program to different areas

	N	Minimum	Maximum	Range	Median	Grouped Median	Variance
29_1 Asset protection	46	2	6	4	5,00	5,00	1,374
29_2 Compliance with laws and regulations	46	2	6	4	5,00	5,06	1,360
29_3 Improved Corporate competitiveness	46	1	6	5	4,00	3,68	2,199
29_4 Increase Customer base	46	1	6	5	3,00	3,10	2,399
29_5 Increased Production	46	1	6	5	3,00	3,38	1,932
29_6 Managing Security Investments	46	1	6	5	4,00	4,17	1,865
29_7 Mapping ICT Business Criticality	46	2	6	4	5,00	4,43	1,438
29_8 Reliable and Secure Operations	46	2	6	4	5,00	5,20	1,088
29_9 Safeguarding Systems	46	2	6	4	5,00	5,21	1,133
29_10 Safeguarding Employees	46	1	6	5	4,00	4,16	2,188
29_11 Security Management	46	2	6	4	5,00	5,00	1,347
29_12 Threat Intelligence	46	2	6	4	4,00	4,30	1,807

4.4 An Initial Insight Into Information Security Risk Assessment Practices [159]

This paper is part two part of a study on the practitioners view on InfoSec issues and reviewed ISRA practices. One of the key contributions from the research 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. 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, whereas low-tier risks were handled on an ad-hoc basis while the level of formality increased with higher abstraction levels.

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.

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 ISRA approaches are qualitative, while those who described their work as more technical were more likely to describe their ISRA 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. These results highlight 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 practitioners seldom apply Black Swan theory 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.

4.5 A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF [161]

In general, an Information Security Risk Assessment (ISRA) method produce probabilistic risk estimates, where risk is the product of the probability of a given occurrence and the consequence of the event for the given organization. ISRA practices vary from industries and discipline, resulting in various approaches and methods for risk assessment. There exist several methods for comparing ISRA methods, but these are scoped to compare the content of the methods to a predefined set of criteria, rather than process activities to be carried out and the issues the method is designed to address. It is the lack of an all-inclusive, comprehensive comparison that motivates this work. This paper proposes the Core Unified Risk Framework (CURF) as an approach to compare different methods. We developed CURF as an all-inclusive (Unified) ISRA model, growing it organically by adding new issues and tasks from each reviewed method. If a task or issue was present in surveyed ISRA method, but not in CURF, it was appended to the model, thus, obtaining a measure of completeness for the studied methods. The scope of this work is primarily functional

4. SUMMARY OF PAPERS

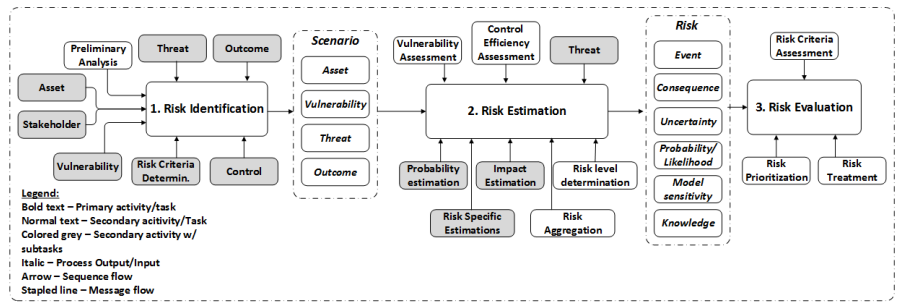


Figure 4.4: Top level of CURF. The generic output of the Risk Evaluation is prioritized risks.

approaches risk assessment procedures, which are the formal ISRA methods that focus on assessments of assets, threats, and protections, often with measures of probability and consequence. This study does not address aspects beyond risk identification, estimation, and evaluation.

The CURF approach allowed for a detailed qualitative comparison of processes and activities in each method and provided a measure of completeness. CURF was developed inductively through reviewing eleven well documented ISRA methods; CIRA [117], CORAS [105, 52], CRAMM [170], FAIR [87, 62], NSM ROS [113], OCTAVE Allegro [46], ISO/IEC 27005:2011 [15], NIST SP 800-30 [37], and ISACA Risk IT[4]. In addition, two domain-specific methods, whereas one for cloud, CRDF [140], and The Norwegian Data Protection Authority's (Datatilsynet) *Risk Assessment of Information Systems* (RAIS) [8]. Fig. 4.4 shows the top level of CURF, with potential inputs and outputs for each process step.

We found the "ISO/IEC 27005 Information Security Risk Management" to be the most complete approach at present, with the Factor Analysis of Information Risk (FAIR) as the most complete risk estimation method. Also, we also discovered several gaps in the surveyed methods. Literature studies show that there exist multiple comparative assessments of ISRM/RA methods, but these are all scoped to compare method contents to a predefined set of criteria, equivalent to a top-down approach. For most cases, this is less flexible concerning addressing issues missing in the predefined criteria. With CURF we have shown the utility of comparing methods and building the framework from a bottom-up point of view. Our results, therefore, consists of a larger superset of issues and tasks from all reviewed ISRA methods using ISO/IEC 27005:2011 as a reference point, and then comparing the ISRA methods as a measure of completeness covering all the issues and activities added to the superset. The possibility to add new problems makes our proposed framework highly flexible to changes in future methods and comparing methods that are very different.

No evaluated method is complete in CURF, but from all of the methods reviewed, ISO/IEC 27005:2011 is the most complete and covers most issues in one way or another. However, FAIR was the most complete method risk estimation. Another finding is that beside FAIR, there is little information on how to obtain quantitative probabilities in any of the ISRA methods reviewed. There are several ISRA frameworks and practices. However, we find variations of asset evaluation, threat, vulnerability and control assessments at the core of the most reviewed frameworks. While the more specific issues, such as cloud risk assessment, is primarily addressed by methods developed for that purpose. It was also interesting to find that none of the ISRA methods discuss the presence of unknown unknowns (Black Swans), which is highly relevant due to the dynamic and rapid changes in ICT systems, which only are growing and getting more complex. Beside CIRA, the human motivational element of InfoSec and ICT systems seems mostly neglected.

4.6 Information Security Risk Assessment: A Method Comparison [160]

Information security risk assessments (ISRA) are performed daily according to different standards and industry methodologies, but how do the choice of method matter for the work process and the results? This research qualitatively investigates the observable differences in effects from choosing one method over another, through four empirical case studies applying each of the three following methods; (i) ISO/IEC 27005:2011 Risk Management Guidelines [15], (ii) OCTAVE Allegro (OA) [46], and (iii) the Norwegian Security Authority Guidelines in Risk and Vulnerability Assessments (NSMROS) [113]. The study first outlines the theoretical differences between the three methods using the Core Unified Risk Framework (CURF). Second, we collected experience data from the risk assessment teams for analysis. Third, we examined the metadata of the produced risk assessments using CURF to explore differences.

Our results show that the choice of ISRA method does matter both regarding content, experience, and yielded results. From applying CURF on each of the three methods, we had knowledge about their theoretical strengths and weaknesses on the beforehand, which also corresponded well to the content of the report. However, there was only partial overlap between the theoretical differences outlined with CURF and the experienced differences. Following our novel application of CURF to analyze metadata, our study found that CURF worked well as a bottom-up approach to establishing a cause-effect relationship between ISRA tasks and produced results. Table 4.2 displays the differences between the initial CURF findings and the metadata in the produced reports. Thus, when inexperienced risk assessors apply a method, what the method includes and does not include matters strongly for the outcome of the risk assessment. Our results show that the choice of method matter for both the work process and the outcome of the risk assessment.

Our analysis of collected experience data showed that the choice of the method does mat-

Table 4.2: Comparison of observable theoretical differences from CURF and differences in reports

Task	NSMROS		OCTAVE A		ISO27005		
	CURF	Report	CURF	Report	CURF	Report	
Case descr.							
Organizational Dr.	0	X	XX	XX	0	X	
Risk Measurement Criteria	X	XX	XX	XX	XX	XX	
Org. Goals/ Business objectives	0	X	XX	X	XX	XX	
Risk Ident.							
Stakeholder Id.	0	XX	X	XX	XX	XX	
Asset Identification	XX	XX	XX	XX	XX	XX	
Asset Evaluation	XX	X	X	XX	X	XX	
Asset Container	0	0	XX	XX	0	X	
Threat Identification	XX	X	XX	XX	XX	XX	
Threat Assessment	X	0	XX	X	XX	XX	
Areas of concern/ Vulnerability Id.	X	XX	X	XX	XX	XX	
Vulnerability assessm.	0	X	0	0	XX	XX	
Control Identification	0	X	X	0	XX	XX	
Control assessment	0	0	0	0	XX	XX	
Outcome identification	XX	XX	XX	XX	XX	XX	
Risk Est.							
Impact Area Pri.	0	X	XX	XX	0	X	
Threat motivation	0	0	XX	XX	XX	XX	
Threat Capability	0	0	0	0	X	XX	
Threat Capacity	0	0	0	0	X	XX	
Qualitative Conseq. Estimation	XX	XX	XX	XX	XX	XX	
Qualitative Prob. Estimation	X	XX	X	XX	XX	XX	
Risk Scenarios	XX	XX	XX	XX	XX	XX	
Risk Matrix/table	XX	XX	XX	XX	XX	XX	
Risk Eval. & Treatment							
Risk Prioritization	XX	XX	XX	XX	XX	XX	
Treatment plan	XX	XX	XX	XX	XX	XX	
Cost/benefit analysis	XX	XX	0	XX	X	XX	
Residual Risk	X	X	XX	X	XX	XX	
<i>Total Results (CURF-Rep.)</i>	<i>Occurrences (Total 78)</i>	XX-XX X-X 0-X	40 1 8	XX-X X-0 0-XX	5 2 2	X-XX 0-0	11 9

ter for the process and the issues the practitioner will be facing during the risk assessment. However, there are ISRA issues that span all the surveyed methods, and these were not uncovered through our CURF comparison of the frameworks. A lot of the feedback on the use of methods was related to user-friendliness and not to process or tasks. Some issues are universal and should be prepared for, such as data collection issues were similar for all groups. Also, the necessity of some tasks for succeeding, such as organizational understanding and stakeholder identification, forced the practitioners to conduct them whether they were present in the framework or not. The participating groups also favored checklists, and the OA groups highly valued the OA worksheets, whereas the NSMROS and ISO27005 groups reported to having spent time looking for examples and checklists. Thus, these are popular items to include into ISRA methods. Our uncovered practical problems should also strengthen the research incentive within specific theoretical ISRA areas, in particular, method development and usability, tools for organizational understanding, asset evaluation, risk estimation, and threat assessments.

4.7 Quantitative Risk, Statistical Methods, and The Four Quadrants for Information Security [162]

Achieving the quantitative risk assessment has long been an elusive problem in information security, where the subjective and qualitative assessments dominate. This paper discusses the appropriateness of statistical and quantitative methods for information security risk management. Through case studies, we discuss different types of risks in terms of quantitative risk assessment, grappling with how to obtain distributions of both probability and consequence for the risks. N.N. Taleb's concepts of the Black Swan [144] and the Four Quadrants [143] provides the foundation for our approach and classification. We apply these concepts to determine where it is appropriate to apply quantitative methods, and where we should exert caution in our predictions. Our primary contribution is a treatise on different types of risk calculations, and a classification of information security threats within the Four Quadrants. For more on these topics, see Chapter 2.8.2.1.

In this paper, we investigated quantitative risk calculations based on the available data. We provided a classification of where it is safe to apply statistical methods and where to expect a reasonable return on investment in improved decision making within the Four Quadrants, Fig. 4.5. The Four Quadrants paper provides part of the foundation for the risk assessment model proposed in the last article. This work studied whether the statistical approaches are feasible to deal with InfoSec risks at all and what are the advantages of using such methods, considering their reliability for the prediction. One can state that conventional statistical methods provide reliable accuracy only in case of significant amount of historical data and when the event in question is located within the tolerance interval from the past data. The implications of the study have discovered severe limitations of quantitative forecasts when it comes to targeted attacks, namely malicious individuals, and sophisticated threat agents. The increase in both complexity and interconnectivity limits our ability to forecast.

4.8 Cyber Security Risk Assessment of a DDoS Attack [163]

This paper proposes a risk assessment process based on distinct classes and estimators, which we apply to a case study of a common communications security risk; a distributed denial of service attack (DDoS) attack. The risk assessment's novelty lies in the combination both the quantitative (statistics) and qualitative (subjective knowledge-based) aspects to model the attack and estimate the risk. The approach centers on estimations of assets, vulnerabilities, threats, controls, and associated outcomes in the event of a DDoS, together with a statistical analysis of the risk. We used CURF to derive the classes and estimators for the qualitative model, while we used the results from the Four Quadrants Paper [162] to

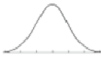
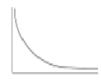
	1 Simple Payoff	2 Complex Payoff
A Mediocristan 	<i>First Quadrant, Extremely safe</i> 1. Hardware and component failure risks 2. Simple user errors 3. Exploiting known vulnerabilities from automated scans	<i>Second Quadrant, Safe</i> 1. Hardware system failure risks 2. Single Malware infections 3. Generic Phishing campaigns 4. Insider attacks 5. Known Targeted Attacks
E Extremistan 	<i>Third Quadrant, Safe</i> 1. DDoS Attacks 2. Self-propagating automated malware	<i>Fourth Quadrant, Black Swan Domain</i> 1. Cascading risks 2. Systemic risks 3. Novel APT / Targeted attacks 4. Terrorist attacks 5. Cyberterror/war 6. Complex Insider attacks (e.g. Snowden) 7. Complex User Errors

Figure 4.5: The Four Quadrants with Risk Classifications. *Based on Taleb[143]*

expand the DDoS model. Our main contribution is the process to combine the qualitative and quantitative estimation methods for cyber security risks, together with an insight into which technical details and variables to consider when risk assessing the DDoS amplification attack. This paper contributes towards making the overall risk assessment process

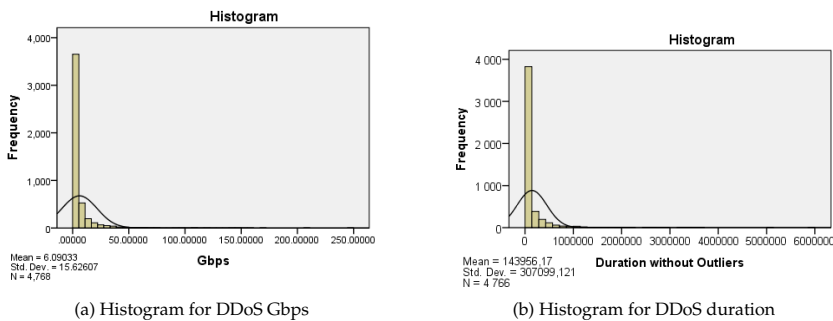


Figure 4.6: Histogram of DDoS magnitudes and durations with normal curve, without two largest outliers. *Data Source: Akamai [19]*

easier and more comprehensive, by showing that applying statistical methods for a cyber risk is feasible as long as there is data available, see Fig. 4.6 for the DDoS duration and magnitude distributions we received from Akamai [19]. Moreover, with more accurate data there are possibilities for even better quality models. Also, we adjusted the quantitative risk estimates with qualitative findings, for example, the definitions of scenario events (A and B) were based on qualitative measures of vulnerability and applied to categorize objective data. This paper also took the merging further by implementing the findings from the qualitative threat and control efficiency assessments into the probabilistic model. The control estimation is crucial to the risk estimation as it directly affects the estimation result, which in our case study made the most severe outcomes very unlikely. The combined qualitative and quantitative risk assessment is displayed in the modified event tree, Fig. 4.7. Thus, the conclusion is that combination of both the qualitative and quantitative

4. SUMMARY OF PAPERS

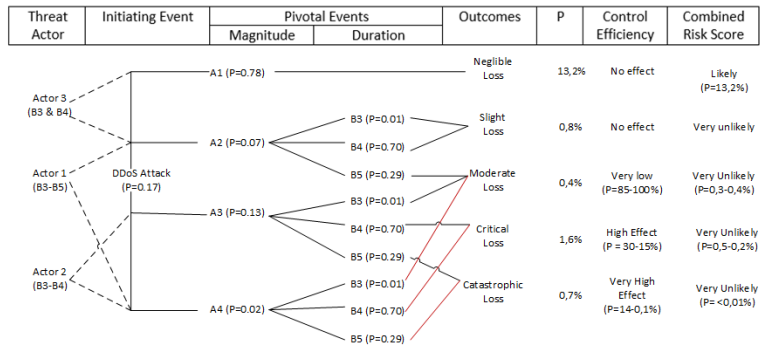


Figure 4.7: Expanded Event Tree also including subjective estimates of threat actors and control efficiency.

aspects of ISRA is both feasible and beneficial. Defining an ISRM method as either-or in this manner may cause the risk analyst to miss out on valuable information for the assessment.

Summary of Thesis Contributions

This chapter outlines our knowledge contributions within the information security risk assessment field. The chapter follows the research question sequence and outlines each research question together with a summary of the contributions. We have divided the contributions into four main areas. Lastly, the contributions are evaluated within the DSR framework.

5.1 Theoretical Insights into ISRM Practices

RQ 1: What are the known theoretical issues in Information Security Risk Management?

One of the research contributions of the thesis is the identification of current research problems together with limitations on the state of the art. The theoretical foundations for the future study was formed through literature review (Article I [164]) and theoretical analysis (Article II [165]). Article I answers the above RQ and has the following contribution:

- Building on the ISO/IEC 27005:2011 process model this article proposes a taxonomy for classifying research problems within traditional ISRM activities.
- Contributes a non-exhaustive overview of known ISRM theoretical research problems within the proposed taxonomy.
- The article provides a foundation for a holistic understanding of underlying causes of prevalent problems within the research area.

RQ 2: How does the overall Information Security Management Frameworks compare with other Business Management frameworks?

For the analytical theoretical comparison, Paper II [165] identifies the key components of three Information Security Management (ISM) frameworks (ISO/IEC27001:2013 [13], ISO/IEC27002:2013 [14], and NIST SP 800-39 [103]) and maps them to established Business Process Management (BPM) approaches (The BPM methodology framework by BPTrends [1] as described by Harmon [70] and Mahal [106]). Article II found that the tasks and goals of each level are similar, with some key differences:

- The primary research contributions from this study was weaknesses and areas for improvement in ISM compared to BPM.
- The study determined that the compared frameworks had a strong similarity and could be integrated as management frameworks.

5.2 New Practical Insights into ISRA practices

Question 3: How does the theoretical ISRA issues coincide with practical issues in Information Security Risk Management?

This study builds on the findings from investigating RQ 1 and 2, and explores the practitioners view of the previously discovered issues and challenges within ISRA, paper [157] addresses generic risk management, while paper [159] addresses specific risk assessment and analysis issues. The specific contributions are:

- New insight into several ISRA and ISRM research problems from the practitioners point of view.
- Identified several new issues and paths for future research.
- Validated and got new perspectives on already known problems.
- Provided basis for future work grounded in both academic literature and experience data.

5.3 The Core Unified Risk Framework (CURF)

Question 4: How does different ISRA approaches compare qualitatively from a bottom-up perspective?

This thesis contributes by developing a new approach for comparing ISRA methods, CURF [161]. The study was motivated by an attempt at building a model for determining cause and effect relationships between ISRA method application and the produced results. We found that the existing comparison approaches first determined a set of criteria for comparison and then scored the reviewed methods on these criteria, which was insufficient for our purposes. Instead of relying on a predetermined set of criteria, we developed CURF as an all-inclusive (Unified) ISRA model. We grew CURF organically by adding new issues and tasks from each reviewed method. If a task or issue was present in surveyed ISRA method, but not in CURF, it was appended to the model, thus, creating a super-set of tasks and issues. This approach allowed us to score each reviewed method on completeness when compared to other methods and their content. We consider the DSR contribution in this study as primarily the artifact, CURF, which entails a method and the application of CURF to produce a knowledge contribution to the ISRA community.

- Developed a novel method for bottom-up and comprehensive comparison of ISRA frameworks.
- Contributed with a non-exhaustive super-set of ISRA tasks and activities.
- Displayed the utility of the framework by contributing knowledge on strengths, weaknesses, and focus areas of the reviewed methods.
- Contributed with a method for deriving a completeness score for ISRA frameworks.

5.4 CURF Applications

Question 5: How does the choice of ISRA method matter for the risk assessment results?

In this study [160], we applied three ISRA methods, each conducted on four case studies, twelve in total. We applied CURF to compare the three methods and the produced results to determine cause-effect relationships. In addition, we gathered experience data from the groups running the risk assessments and compared the experiences with each method.

- Documented knowledge and experience data on conducting risk assessments using three different methods.
- Novel application of CURF as a method for establishing causality between ISRA method and produced results.
- Established causality between choice of ISRA method, work process, and risk assessment results, including evidence that choice of method matters strongly for the outcome of the assessment.

- Developed a method for comparing risk assessment meta data which opens a new research area of practical ISRA comparison.

Question 6: What are the requirements and limitations for constructing a hybrid risk assessment model?

Our prior research with gathering practical and theoretical insights in ISRM revealed the application of statistical method and risk quantification is one of the most heavily discussed problem in ISRM. This research explored the limitations of statistical methods for ISRA [162], before proposing a *Hybrid* (combined Qualitative and Qualitative) risk assessment model grounded developed by applying CURF.

- Defined limitations of statistical models for ISRA by exploring the Black Swan concept [144] and adopted Taleb’s four quadrant risk assessment model [143].
- Defined several factors that may lead to unpredictability of InfoSec risks and risk classification for applying probability distributions in InfoSec.
- Demonstrated a novel application of CURF for building risk assessment methods from the reviewed methods.
- Proposed a novel hybrid risk assessment model for assessing DDoS attacks based on CURF. Which combined quantitative probability distributions with subjective knowledge for risk calculations using modified Event trees.
- Contributed knowledge on how to risk assess DDoS attacks.

5.5 Evaluation of Artifacts

Table 5.1: Evaluation of Artifacts

Artifacts	Goal	Contribution	Evaluation Metrics	Evaluation Method
Construct 1	Identify and categorize ISRA problems, determine relevance, and form basis for ISRA models.	Taxonomy of Challenges for ISRM [164] A Comparison between BPM and InfoSec Management. [165]	Relevance, Completeness	Expert validation and Evaluation [157, 159]
Construct 2	Identify limitations of quantitative risk prediction for ISRA, classify, and use for ISRA model development	The Four Quadrants Classification of InfoSec Risk [162]	Feasibility Suitability	Descriptive Informed Arguments, Scenarios, Simulation, and Model development [163]
Method and Model 1	Develop a method for bottom-up comparison of ISRA methods and a measure of completeness, and model the findings	CURF [161] <i>Method:</i> Bottom-up comparison and completeness <i>Model:</i> CURF Data model	Completeness Relevance	Testing, Incremental improvement, and Demonstration [163, 160]
Method and Model 2	Develop a ISRA method and model that combines quantitative and qualitative estimations	Cyber security risk assessment of a DDoS attack [163] <i>Method:</i> Qualitative and Quantitative ISRA approach <i>Model:</i> Expanded Event Tree	Usability Relevance	Testing and Observational Case study
Method 3	Develop a method for comparing ISRA results	An Empirical study of ISRA Methodologies [160] <i>Method:</i> Comparison of ISRA Metadata using CURF	Relevance Usability	Dynamic analysis and Testing

Artifact evaluation is one of the key activities in the DSR methodology [75] and this section categorizes and describes the evaluation method for each developed artifact. This Thesis proposes many artifacts, of which two constructs, two combined methods and models, and a third method. Table 5.1 categorizes the artifacts, describes goal, contribution, evaluation metrics and method.

Construct 1: Articles I [164] and II [165] introduces the construct for categorizing and understanding the problem space. The evaluation of the construct was done with an online-questionnaire in Articles III [157] and IV [159] evaluating the relevance and completeness of the construct. The expert studies ([157, 159] evaluated how relevant each of the proposed problems from the initial taxonomy was for their work environment by using the rating and ranking questions. We evaluated the completeness of the construct by having multiple open-ended questions and comment fields for the respondents to give their opinion and propose additional issues or research areas. The respondents contributed new problems adding to the completeness of construct.

Construct 2: The second construct is proposed in Article VII [162], which applies the Four Quadrant risk classification system [143] as a feasibility study for typical InfoSec risks. The study analyzes the suitability of common statistical analysis methods for these risks and identifies which factors that limit forecasting ability. For evaluation the study primarily used case studies and scenarios, which was built with either existing data-sets or simulated datasets from relevant data points. Descriptive Informed Arguments as an evaluation form in which the authors identified forecasting limitations and built an argument for the utility of the Four Quadrants.

Model and Method 1: The first Method and Model we propose in this Thesis is in Article V [161], CURF, in which the DSR *method* is the bottom-up comparison approach. The DSR *model* is the Data model (for example Fig. 4.4 in the previous chapter). For CURF, completeness and relevance were the evaluation metrics. In which, we evaluated the former through continuously testing the framework, using incremental improvement by adding new methods to the framework until the activity categories started saturating and return on investment went down. We demonstrate the utility of CURF by evaluating the completeness of the surveyed methods, comparing risk assessment results [160], and utilizing the findings from CURF to model the risk of a DDoS attack [163].

Model and Method 2: The second Method and Model contributed in this Thesis is a hybrid ISRA method and model [163], which was evaluated it trough a case study. We considered relevance and usability as the two evaluation metrics for the hybrid ISRA model; both evaluated through the application of the method and model to a real case study.

Method 3: The third method we introduce in this Thesis is a development of CURF in which we applied it to compare ISRA method application and results [160]. This study evaluated the usability by applying the method to a set of collected data (ISRA results) and establishing a cause-effect relationship. We analyzed the results in order to evaluate if the method had relevance to the investigated problem.

5.6 Summary of Contributions within the DSR Quadrants

This Thesis provides five DSR contributions, Table 5.1, the following text analyzes the contribution and positions them within the DSR knowledge contribution framework [67]. Figure 5.1 summarizes the contributions within the four DSR quadrants.

Starting with the first construct, the Taxonomy of Challenges for ISRM [164], which is a classification of documented research and practical problems. Classifying data is a known problem, and the Taxonomy is a new solution, which places it in the *Improvement* category. The second construct is the Four Quadrants classification of InfoSec risk [162]. In which we extended a known solution, Professor Taleb's four quadrants [143], to a new problem, namely risk classification for forecasting in ISRA. Which places the Four Quadrants in the *Exaptation* quadrant.

The first method and model are CURF [161], in which we developed a bottom-up ISRA method classification and comparison framework for estimating completeness. According to our literature review, the bottom-up comparison was novel for ISRA methods. The problem of estimating method completeness was also novel, which places CURF in the *Invention* quadrant.

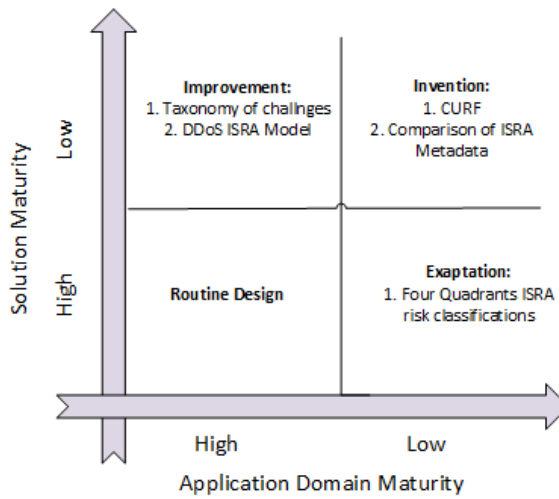


Figure 5.1: DSR Knowledge Contribution Matrix for this Thesis

The second method and model is our hybrid ISRA of the DDoS attack [163]. Risk assessing DDoS attacks is not a novel problem, however, the ISRA model is novel. Which makes the hybrid model a new solution to a known problem, placing it in the *Improvement* quadrant. Lastly, the third method is a development of CURF in which it was applied to compare risk assessment results. Which was a novel problem that required a modified CURF approach, placing the contribution in the *Invention* quadrant.

Future Work

This work has addressed several issues in ISRA and produced several opportunities for future work. This chapter starts with a discussion of future directions for CURF. Secondly, we discuss the research areas we explored in ISRA method application comparison. Thirdly, we provide research directions for our CURF-based risk assessment method. Lastly, we address potential areas for future work uncovered in the literature study and survey.

6.1 Future directions for CURF

Currently, CURF has limitations in the abstraction layer as we chose to keep the comparison at a high-level and the model does not display deeper differences between methods such as specific approaches to asset identification, vulnerability assessments, and risk estimation. For example, the new version of FAIR [62] comes with a detailed approach to risk estimation, while other methods that appear somewhat equal in the comparison, such as NSMROS [113], only describes the activity with at a high abstraction. A closer study of the methods and a possible expansion of the tables will reveal deeper differences in scope and methodology not present in our work, which includes the time-parameter for PxI calculations. A possible addition to the framework is to expand it with experience-based knowledge and to grow it by making it available to other scholars and practitioners. Comprehensiveness of activities and accessibility of the ISRA methods is not entirely considered in this comparison, which are issues we uncovered for some of the frameworks. Our research [160] found that accessibility is one of the most desirable components of a framework for ISRA novices. Which makes adding these two components to CURF a path for future work.

Another limitation is that, although, for example, ISO 27005:2011 scored low on the cloud specific criteria, third party management is covered in the supporting material (ISO/IEC 27001 and 27002 standards). This may also be true for other reviewed methods.

Further, this work highlights the need for a more thorough discussion on what the different aspects of an ISRA should consist of, such as threat and control assessments. Another path for future development of CURF is to operationalize it and make it available to the ISRA community. One possible way of achieving this is to create supporting software and make it accessible on the Internet for professionals to add and edit methods and tasks. Related to this direction are studies of cost-effectiveness for ISRA methods, at the moment, we have over one hundred different available methods to choose from [127], but there is a lack empirical data on what works within these approaches. CURF could facilitate such a large-scale comparative study and provide the knowledge basis for a larger community of practice for ISRA.

6.2 New research area in method comparison

By applying CURF, we enabled an empirical comparison of ISRA method content and produced results. This novel application of CURF opened up a new venue for research into ISRA. One limitation of this study was that we had different case studies for each group, which limited our ability to isolate the method variable regarding ISRA results. With more

resources available for a new study, the researchers can overcome such a limitation by designing the study from start to end. Rajbhandari and Snekkenes proposed case-study role-play for risk analysis research [119], which is an approach that could be tested in combination with CURF for method comparison purposes as well.

Another limitation of our data was that they were gathered from novices and may not apply for specialists and experts. However, we know from experience that on-site personnel and non-specialists often conduct ISRA, for whom, the method is essential, and our results do apply. Using students has its limitations; first, they have diverse interest and ability, which determines the quality of the result. Secondly, most of the groups needed guidance to complete the assignment, which may lead to supervisors influencing the results. Future paths for research in this area would be to isolate the expertise-variable in experiments to judge how much it influences the outcome of the risk assessment.

The sample size is an issue in resource intensive qualitative studies; although the results were strongly indicative, four reports per method may not be enough evidence to conclude. Another path is to reproduce this research to provide more evidence for or against the hypothesis that method choice matters for the risk assessment outcome.

We saw from analyzing the risk assessment reports in this study clear differences between the different tasks proposed by each method. Although describing the same tasks, some task descriptions produced visibly better and more relevant results than others. A path for future research is to look into these differences between methods to derive the most functional parts of existing methods to create a cost-effective and high quality approach to ISRA. Our research uncovered several common denominators for applying all the methods, whereas data collection is the most crucial for the ISRA. A path for future research is studies of data collection methods and techniques for making the ISRA more efficient.

Since CURF still is an innovative approach and not fully developed, further development and expansion of CURF is also possible. We showed in the report assessments that the model is adaptable. However, the idea of CURF can be applied for other comparisons and expanded further by adding more nodes in the tree, for example, expanding with the issues uncovered through practical experience. Also, the CURF idea is also applicable to other frameworks from the management disciplines. Lastly, we encourage others to conduct similar studies, and these will benefit the ISRA community by determining what works and what does not.

6.3 Opportunities in risk prediction and modeling

The increase in both complexity and interconnectivity limits our ability to forecast, and the four quadrants map for information risk is a map for prediction. In which, several of the risks may move between the quadrants when reduced uncertainty with each risk. The four quadrants map can be expanded by analyzing and adding InfoSec risks to increase the value of the heuristic.

In Section 6.2, we proposed to research the most functional parts of the existing methods to derive the most functional parts and construct an ISRA model. We partially did this using CURF to propose our combined quantitative and qualitative risk model. However, there is still much room for improvement: Consider that we constructed CURF by reviewing only eleven methods out of the over one-hundred available [127].

However, there is also a limitation in our model due to the combination of the subjective and statistical assessments. We believe that application of possibilistic models such that Fuzzy Logic may help to understand the reasoning of statistical models better when the probabilities of two events are nearly equal and are very small. It means that the difference between two similar events can be below the limit of computing error because the event falls under the category of what Taleb defines as *Extremistan* (see [144, 143]). Therefore, applying a combination of subjective and objective estimators, we will be able to achieve better generalization of the model. Another way to improve the methodology is to use

hierarchical models that ensemble inference of human-understandable Fuzzy Rules (also used for decision support) into a comprehensive framework.

We propose to apply our approach to model other cyber risks for further validation. The risk considered in this paper is a very technical communications risk, and the risk model would benefit from testing and development in areas where historical data is less available. Our model can also be expanded and tested using the Cyber Security measurement methodology proposed by Hubbard and Seiersen [82].

Another limitation is the limited generalization of our case study; the ISRA approach should also be applied to other types of organizations. 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.

6.4 Future directions in generic ISRM/ISRA

Firstly, the Taxonomy of challenges for ISRM highlighted many areas for future work, most of which are still relevant. The Taxonomy itself can be further expanded and elaborated by adding new research findings to the classification, including the findings from research presented in this Thesis. This would benefit the ISRA research community by having an updated research menu to chose from.

Our comparison study [165] and the survey with the ISRA practitioners [157, 159] revealed several interesting paths for future research: we found stakeholder management lacking in information security. 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 addition, we found that measuring security is one of the most challenging aspects of InfoSec. Hubbard and Seiersen [82] has recently published a book on measuring InfoSec risk, and empirical studies of the proposed method is an interesting venue for further work.

Another issue we found was that ensuring buy-in and maintaining continuous funding for InfoSec projects, together with visualizing the benefits from the ISRM program, was key issues the practitioners faced on a daily basis. Which highlights the need for risk communication and rhetoric skill training in future InfoSec training.

Another path for research is risk assessment application through the organizational tiers. We found that some organizations vary their approaches according to tiers, but more research is needed to determine whether this has any merit, and to derive potential benefits. As a future direction, we propose to research handling and assessing risk between the organizational tiers, together with risk escalation issues.

Composition and optimization of the ISRA team from the knowledge perspective is a potential path for future research. Quantification of risk A path for future work is to research the intersection between these two approaches to optimize the ISRA results.

Conclusion

The pressure to digitize and automate in today's and tomorrow's business environment will increase the need for ISRM programs in the years to come. This development will also put pressure on the InfoSec departments to document their contributions in competition for funding. Being able to estimate risk enables us to make better security decisions which are where this Thesis aimed to contribute. Throughout the research, we have contributed with novel research problems, methods, models, and knowledge to improve ISRA practices and research. The following text concludes the work:

The research began with theoretical studies which contributed to the structuring research related information in the ISRM/RA field. We presented a taxonomy based traditional ISRM activities, for the purpose of classification of challenges within the ISRM area of research. Which also contained a non-exhaustive backlog of problems that exist within the research field, and classified within the taxonomy. We have also identified a collection of significant challenges that are prevalent in ISRM and provided a foundation for a holistic understanding of underlying causes of problems. To add the understanding of ISRM/RA we compared it to BPM frameworks and found a strong similarity between them. However, our work also highlighted differences and potential shortcomings. Together, these two studies [164, 165] provided a comprehensive knowledge basis for further studies of the area, and our survey with the ISRA practitioners was designed using findings from it. The survey provided an initial insight into the InfoSec risk practitioners view of ISRM/RA. Although our survey did not produce as many respondents as desirable, we got several high-quality responses that provided opinions and insights into different research areas. The findings from the survey also validated several research problems that were later pursued during this research, especially method application and risk quantification.

Perhaps the biggest innovation in this Thesis is CURF. The invention of CURF was necessary to enable the comparison of the risk assessment reports for Paper six, but it turned out to have other useful areas as well. The comparisons and completeness scores in CURF all have utility, for example, by aiding practitioners choose method or developers looking for areas of improvement for their methods. The idea of the bottom-up comparison for frameworks is also applicable to other research fields.

CURF showed utility when we compared three sets of ISRA reports produced with different approaches. Our study found that the choice of ISRA method does matter both regarding content, experience, and produced results. Our novel application of CURF to qualitatively analyze metadata worked well to establish a cause-effect relationship between ISRA tasks and results. Besides, we found a clear relationship between method and report completeness, whereas the ISO27005 groups scored highest. From this study, we could conclude that when inexperienced risk assessors apply a method, its content matters strongly for both the ISRA process and outcome. Just as significant a contribution was the approach to comparing metadata, which enabled us to find these differences.

As one of the most pressing issues we found in the literature was risk quantification, the research moved towards this area. Instead of directly attempting to quantify risk, we researched the limitations of statistical forecasting using Black Swan Theory. The four quadrants classification of where it is safe to apply statistical methods and where to expect a reasonable return on investment in improved decision-making provided the frame for this work. The article has presented several major cases within the Information Security area,

7. CONCLUSION

with a corresponding applicability study of statistical methods. Our initial risk analysis of the DDoS attack placed in the third quadrant, as it was feasible to obtain distributions of occurrence, magnitude, and duration. The generic consequence of such an attack could also be estimated by considering the loss of availability. Because of these reasons, the DDoS attack was an ideal candidate for further risk modeling. Thus, we applied for our review work with CURF to make a risk assessment model of the DDoS attack by combining qualitative and quantitative estimations. Our work shows that applying statistical methods for a cyber risk is feasible as long as there is data available. Moreover, with more accurate data there are possibilities for even more accurate and better quality models.

Part II

Published Research Papers

Article I - A Taxonomy of Challenges in Information Security Risk Management

Gaute Wangen & Einar Snekkenes

A Taxonomy of Challenges in Information Security Risk Management. Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2013 - Stavanger, Akademika forlag, 2013, 2013.

8.1 Abstract

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

8.2 Introduction

The main goal of information security (IS) is to secure the business against threats and ensure success in daily operations[10] by ensuring confidentiality, integrity, availability and non-repudiation. Best practice information security (IS) is highly dependent on well-functioning risk management (RM) processes[36, 155], and RM is often viewed as the cornerstone of IS[167]. Information security risk management (ISRM) is the practice of continuously identifying, reviewing and monitoring risks, to obtain and maintain risk acceptance[15].

ISRM is a complex field with many unsolved problems; some make the claim that the current state of risk management is that it is broken and does not work[85], while others take it a step further and claim that the current qualitative risk management practices are actually worse than having nothing[80]. We believe that an understanding of the underlying reasons that are causing problems is essential for the scientific community and industry to be able to make progress. Due to the complexity and interconnections in the research field, researchers should avoid addressing one isolated problem at a time while ignoring the remaining challenges. However, the known problems in the ISRM research field are not easily visible being dispersed throughout the scientific literature. There is therefore a need for an overview of the current problems and challenges in the discipline to support a more holistic approach to ISRM research.

In this article, we have collected a non-exhaustive compilation of ISRM and Risk Analysis (ISRA) problems highlighted in published literature. We present a taxonomy based on current best practices for ISRM to aid in identifying prevalent problems, and for sorting current challenges in the research field. This article will therefore be useful in a setting

where the reader need an overview of the current issues in the research field and of the known theoretical causes of problems in the ISRM practice.

We organize this article as follows. In section 8.3 we introduce existing works on ISRM taxonomies. Section 8.4 describes our taxonomy of ISRM challenges and findings. Section 8.5 contains a discussion and analysis of the results, and section 8.6 states the conclusion.

8.3 Related Work

Syalim et.al. [142] provides a comparison of four established risk analysis methods. As a basis for comparison, the paper provides four basic steps of risk analysis, being Threat identification, Vulnerability Identification, Risk Determination, and Control Recommendation. The framework proposed by Bornman and Labuschagne[38] was created to aid organizations in choosing a ISRM method. The comparison uses detailed versions of three criteria; Risks, Management and Processes, which in short represents what, who and how. Ekelhart et.al.[56] highlights the need for a security ontology, a "common language" for IS professionals to ease communication and help achieve a common understanding of IS across companies and borders. Another purpose of the ontology is to improve the existing quantitative risk analysis. "The Risk Taxonomy" is a technical standard provided by the Open Group[9], and is a document that offers a standard definition and taxonomy for IS risk to help combat the growing language gap between professionals. It also provides a model that contains a set of requirements and factors that all new risk assessment approaches should include.

Behnia et.al.[34] has published a survey of ISRA methods, which also contains a comparison of several of the popular ISRM methods. The presented framework for comparison is based on criteria such as if the method has supporting tools, vendor name, country of origin, etc... The purpose of this comparison framework is to assist practitioners in choosing an ISRM for his organization.

ENISA[2] rate several different ISRA approaches according to quality. The report also contains an overview of methods that contain ISRM steps. ENISA also addresses the skills needed for conducting each method.

Campbell and Stamp[44] present a classification scheme where ISRM methods are sorted in a 3-by-3 matrix. The scheme sorts methods by level of detail and type of approach. This scheme provides practitioners an inkling to what skill level is required, intrusiveness, and the kind of method (e.g. compliance testing or audit).

Snekkenes[133] presents a taxonomy of ISRM methods using the view of key building blocks in ISRM methods. The taxonomy sorts ISRM into five activity classes for distinguishing and comparing methods. Snekkenes also presents a research menu for ISRM issues and research challenges.

8.4 A Taxonomy of Challenges

The main purpose of our taxonomy is to categorize and present findings at different stages in the ISRM areas and activities. Several of the existing ISRM/ISRA taxonomies have been made to help professionals choose method[38, 34, 2, 44], while others exist to improve certain research problems[9, 56], and for comparison of methods[133, 142]. The taxonomy presented in this paper was created reusing some of the criteria from ENISA[2], together with information collected from the scientific literature survey of existing ISRM methods and frameworks (such as[15, 4, 55] and many more). The main classifications chosen for our model are steps that are present in some form in many ISRM models. The taxonomy includes all the ISRM steps from ISO/IEC 27005:2011[15], and we have chosen to use the vocabulary established by ISO/IEC[10]. The taxonomy is presented top-down model using levels and is illustrated in figure 8.1. We have grouped similar findings within each category.

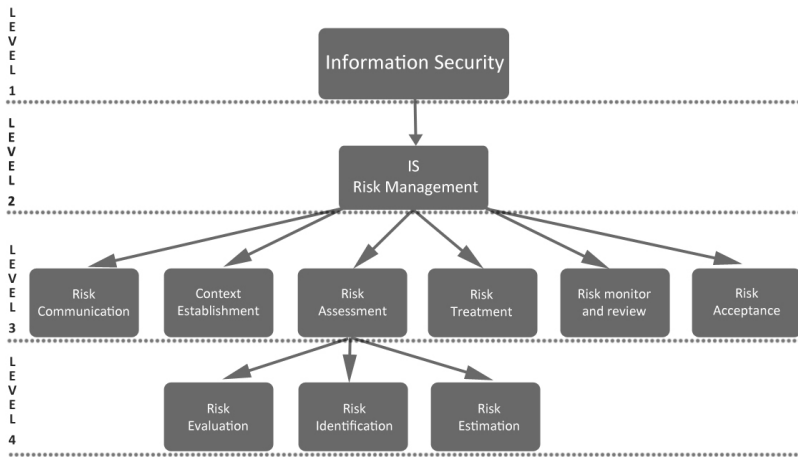


Figure 8.1: The Taxonomy of Challenges in ISRM

- **Level 1, The Information Security Category:** This category contains high-level findings in information security that affect ISRM, these findings did not fit sensibly into the taxonomy because of being a more wide spread issue.
- **Level 2, The IS Risk Management Category:** This category contains general findings in ISRM/RM that did not fit into any of the RM activities in level three of the model.
- **Level 3, The Different Risk Management Categories:** This level contains a classification for all of the identified ISRM activities (see figure 8.1). The findings from the survey are categorized within the activity that they are performed.
- **Level 4, The Risk Assessment Category:** This level contains the findings for the risk assessment category, sorted in the two risk analysis activities "Risk Identification" and "Risk Estimation", and "Risk Evaluation".

8.4.1 Level 1, Information Security

Biased Scope and Misconceptions

Blakley et. al.[36]claims that the discipline of IS is generally more concerned with technical security, which can represent a problem as technical security only represents a small part of the IS risks. Siponen[130] claim that traditional ISRM methods have been dedicated to evaluating technological aspects and to some degree disregard risks within human performance. Which makes it a challenge to detect and treat risks within human performance, human errors, and organization wide factors[35]. While Ozkan and Karabacak[115] point to a similar misconception: such as IS being a purely technical task that can be successfully performed by the IT department only, IS is company-wide and the IT department in general does not have sufficient power to run such a program and seldom have a holistic view of the organization. The same authors also highlight the misconception that consultancy firms can and should achieve IS management for an organization.

Common IS Language

Ekelhart et.al[55] highlights the need for a common IS language, as the language gap leads to confusion among experts, the people and organizations. The Open Group[9] also comments on the language gap that has evolved between businesses, and state that a common,

logical and effective understanding of the fundamental IS problems are required in order for the IS profession to evolve significantly.

Conflicting Incentives and Human Factors

Hagen[69] points to the lack of incentives to report incidents which present a problem in IS. The people that incidents happen to (or cause them) may have many incentives not to report them, leading to underreporting and lack of knowledge regarding the effectiveness system controls[69, 36].

Hubbard[80] comments on the development gap between RM methods, and refers to the problem as a lack of communication between developers. Another problem identified by Hubbard is what he refers to as the over selling of methods that have no proven effect driven by a financial incentive and undermining more theoretical methods that work[80]. The "perverse" economic incentives is also commented on by Anderson[21].

Lack of Empirical Research and Good Data

The majority of the relevant IS and ISRM literature is based on opinion, anecdotal evidence, or experience[97]. Blakley et. al.[36] explains that ISRM professionals do not have sufficient training to design experiments and publish results. The difficulties in obtaining empirical data and conducting IS research is also because of IS being one of the most intrusive types of research that can be conducted[97].

Lack of Validation and Testing

Blakley et.al. [36] states that there is little or no independent testing of IS measures and controls, which leads to lack of knowledge regarding the effectiveness of security measures. Not sharing test data leads to lack of available data for others, and "...the results of effectiveness testing done by vendors and their contractors are almost never published"[36]. Blakley et.al. further claim that security technology has a low effectiveness. Hubbard[80] points out that the methods that are developed lack rigorous scientific testing or mathematical proof.

8.4.2 Level 2, ISRM

Biased Scope and Misconceptions

Harris[71] points to the tendency of practitioners to have a technical scope and focus more on applications, devices, viruses and hacking. She also states that not enough practitioners understand RM and are able to calculate risks and map them to business drivers.

Jaquith[85] points to some misconceptions in mainstream ISRM. He states that the current practice in ISRM misses the important parts and purpose of RM, which are quantification and valuating risk. For most people RM really means "Risk Identification", and that many view security as a product, while it should be viewed as a process.

The "Something is better than nothing" is according to Hubbard[80] a misconception. He further explains that having something is not always better than having nothing. If the organization can not prove that the ISRM program works, it may be worse than having nothing. Money and resources are spent on something that can have zero impact on the organizations business, and failed ISRM may even leave the organization worse off than it was to begin with.

Existing RM methods

Subjective Scoring Methods and Risk Matrices have been claimed to add their own sources of error in an ISRM[80, 22]. Such as compressing ranges[22], *presumption of regular intervals* e.g. different people at different levels in an organization will rate scales differently[80], and *presumption of independence* between risks, some risks are more likely to happen together, and may together present a risk of higher magnitude[80]. Campbell[42] further critic scoring methods that multiplies results, and states that a high-impact low-probability risk is not the same as a high-probability low-impact risk.

There also exist methods that have moved away from using probabilities/likelihood, there exists critique of this as the method no longer is a forecasting method, and cannot be used for "*prediction of probable consequences of action*"[80].

Shedden et. al.[129] comments that traditional checklist-based methods have a too generic

and limited perspective, and that they fail at effectively tying the assessment method to the business. She also claims that established ISRM methods have limitations in viewing people as assets, by not making the distinction between protecting the person and the knowledge.

Lack of Empirical Research and Good Data

Hubbard[80] state that if RM worked the way it was supposed to, a RM program would provide better IS and regulatory compliance records than companies in their peer groups that lack such programs. There would be a clear difference in performance, but there exists no valid evidence to support that ISRM improves corporate performance[80]. Gregory[68] claims that threat forecasting data is sparse, that there is a lack of data on the topic of cyber-related risk, and a lack of understanding of the existing data from a statistical perspective.

8.4.3 Level 3, Context Establishment

Lack of Validation and Testing

Zhiwei[173] points to a lack of analysis and judgment to the overall development tendency of risk evaluation. While Hubbard[80] claim that component testing and completeness checks are virtually non-existent in ISRM methodologies.

Organizational Disconnect

Jaquith[85] claims that viewing security as a product and not a process causes organizational disconnect in spending. He elaborates that spending money on independent security products outside of organizational context is not likely improve security. This view is further strengthened by Zhiwei[173] who claims that risk evaluation methodologies "*fail to take function and goal of information systems in the organization into consideration, which indicates that the basic problem of why to carry on risk evaluation has not been solved*"[173]. Zhiwei further claims that safeguarding information should not be the main target of information security it should be to guarantee the reliability and security in the operational processes and goals in the organization.

Ozkan and Karabacak[115] points to the lack of knowledge from IS/IT professionals regarding the intersection between business and IT processes as being a problem, a risk assessment will lack completeness and produce erroneous results if the practitioners do not have a firm grasp of the business processes.

Another cause for organizational disconnect in ISRM mentioned by Ozkan and Karabacak[115] is when the IT-department are being the drivers and doers of ISRM and ISMS work. *Not realizing that information security is a corporate governance responsibility* is also coined as one of the ten deadly sins of IS[155].

8.4.4 Level 3, Risk Communication

Risk Vocabulary

There are several examples of ISRM professionals not speaking the same "language", a quick look at ISRM standards and frameworks reveal that many use their own definitions of risk [85]. One example of this provided by Hubbard[80] is the definition where risk can be perceived as a good thing; Hubbard claims that the positive outcomes from risks are covered by uncertainty (which is also a word that holds different meaning to different people[80]). In contradiction to Hubbard, David Hillson[77] argues that the common usage of the word *risk* sees only downside. Risk is according to Hillson *the uncertainty that matters*, and adds additional risk treatment strategies for handling "opportunity risks". Lack of a common language for IS risk professionals is a major factor that slows down progression within the research field[80, 9, 56].

There also seems to be some confusion regarding the terms "probability" and "likelihood", some standards use these terms interchangeably[4, 15], while there are other instances where likelihood represent the softer subjective approaches and probability represents quantitative numbers[99].

Interpretation of subjective wording is Another source of confusion pointed to by Campbell[42]. An example of this is one person's "trivial" injury can be another person's "minor" injury, this problem is also mentioned by Hubbard and Harris[80, 71].

8.4.5 Level 3, Risk Treatment

Biased Treatment Strategy

According to Blakley et. al.[36], risk treatment strategies applied in IS primarily focus on risk mitigation. Transference, acceptance and avoidance are alternatives that are seldom considered. The authors further claim that IS as a discipline focus more on reducing the probability of an event than on reducing its consequences.

8.4.6 Level 3, Risk Acceptance

Biased Decision Making

Hubbard[80] points to mistakes in making the assumption that the decision maker is "risk neutral", when few or no people are truly risk neutral, and further claims that how much a decision maker values a risk depends on his/hers risk aversion.

8.4.7 Level 3, Risk Monitoring and Review

Lack of Validation and Measuring

Campbell[42] questions the credibility of subjective/qualitative risk assessments. While Hubbard[80] goes further and claim that new qualitative RM/RA methods do not work. Hubbard claims that RA/RM methods do not account for all the sources of errors in an organization, and some even add their own error, and states: *"Except for certain quantitative methods in certain industries, the effectiveness of risk management is almost never measured"*[80]. Hubbard further points to the lack of objective measurements of risk and validation of RM programs, together with the lack of confirmation of a program really works or not.

8.4.8 Level 4, Risk Identification

Assets

Both Ozkan et.al.[115] and Jaquith[85] point to asset evaluation as a challenge. Putting monetary value on something such as an intangible asset presents a major difficulty, as assets are often dynamic entities that change regularly. However, failing to recognize intangible assets in a RA will cause the assessment to be incomplete as they represents the social and non-technical dimension in an organization. Shedden et. al.[129] make a similar point regarding assets and claim that the current view of ISRM is too technical when it comes to assets. She also points to the problem that the view one takes on assets will affect the risk profile of assessed organization.

Zhiwei[173] critiques the asset-based approach by claiming that protection of assets is not a primary goal of organizations, and claims that protection of the reliability and security in the organization's business processes should be the main goal of IS.

Missing important risks

The current practice of ISRM evaluates each risk on its own and therefore misses correlations between risks states Hubbard[80], e.g. two or more risk events being tied together and creating a domino effect when one risk materializes , and calls this "Cascading risk". Hubbard also explains another concept he claims current RM misses, "Common Mode failure", is when one risk damages more than one system at a time. Hole and Netland[79] claims that traditional ISRM methods underestimate the risks of large-impact, hard-to-predict, and rare events in information systems, so called "Black Swans".

8.4.9 Level 4, Risk Estimation

Lack of Empirical Research and Good Data

Blakley et.al.[36] suggest a connection between a rapid increase in threats and vulnerabilities and a constantly evolving threat picture leading to lack of quality historical data and difficulties in quantitative data collection.

Qualitative Risk Analysis

Several authors claim that the applied qualitative methods are often untested, and we have little knowledge about the effectiveness of the controls we implement to mitigate risk[71, 80, 36]. Harris[71] states that the Qualitative risk assessments and its results are subjective and opinion-based, and involves a high degree of guesswork.

The subjective values eliminates the opportunity to create a dollar value for cost/benefit discussions, which makes it hard to develop a security budget from the RA results[71]. Because of the lack of standardization, each vendor has its own way of interpreting the qualitative processes and their results[71].

The dependence of expert predictions for the qualitative ISRA makes risk estimates for security events unreliable and opens for abuse of the ISRA to fit one's own agenda[35]. Another point of criticism of applying the expert prediction is that it has been proven that people are generally not well calibrated to estimate probabilities[128, 80, 132, 131]. Another criticism of the subjective likelihood scale is that Campbell[42] claim that there is no way of telling the relationship between numbers once it has been converted into the subjective scale.

Quantitative Risk Analysis

Several authors[71, 115, 148] claim that trying to use mathematical formulas for the calculation of risk is confusing, too much work, complex, time consuming and that it requires more preliminary work. Gregory[68] state that the reason for this is that it can be difficult to ascertain reasonable probabilities of threats and their financial impact, and reserves the usage of this method for the highest risk areas. Harris[71] claims that there exists misconceptions about quantitative analysis being purely objective and scientific, and state that it is hard to avoid some degree of subjectivity when it comes the data. Harris further claim that there is no standardized approach to quantitative ISRA, and that each vendor has its own way of interpreting the processes and their results.

There is also criticism claiming that the current quantitative ISRA methods misses the point by not addressing how to calculate probability[99, 123]. They claim that the general description of quantitative ISRA methods are either as SLE or ALE (single and annual loss expectancy) or both, both of which are dependent on probabilities, but they do not address how to calculate the probability itself. Several other sources also point to the difficulty of calculating probabilities without having quality historical data available[35, 151, 104, 68].

Risk Perception

Loewenstein et.al[104] explains how risk analysts are affected by their feelings when analyzing a risk. It has also been proven that risk is perceived differently by genders and races[73], and that different people at different levels in the organizations perceive risk differently[97]. Hubbard[80] claims that subjective risk perceptions are also victim to certain aspects of human nature. Such as the tendency of being overconfident in one's own estimates, and human experts also, tend to make consistent types of errors in judgments about uncertainty and risk, such as underestimating risk. People can also develop tolerance to serious risks after experiencing near misses on several occasions[80]. Peoples' ability to estimate is also inconsistent[80].

"Framing" is a concept that illustrates that the way people are asked a question affects how they answer it[150]. This also applies to risk management[80, 133], where framing of a risk might bias the decision maker.

8.4.10 Level 4, Risk Evaluation

ALE (Annual Loss Expectancy) and SLE (Single Loss Expectancy) Criticism

There exists several points of criticism to ALE and SLE. Jaquith[85] claims that ALE does not work and presents several problems with the approach: The inherent difficulty in modeling outliers, and it is difficult to model a typical loss event. Another reason is *"the lack of data for estimating probabilities of occurrence or loss expectancies, and the sensitivity of the ALE model to small changes in assumptions"*[85]. The author further claims that using averages adds error because real events tend to cluster at the extremes of the scale.

ALE and SLE reduces risk into a single number (vector), by multiplying them together. This does not allow for ranges e.g. for losses (as damage from a fire might result in various losses). Risk is both the probability and the consequence, and should be represented as multiple vectors[80].

Ekelhart [55] comments that the concrete calculation of ALE is dependent on expensive expert knowledge, which is not available to small and medium sized enterprises. Ekelhart also comments on the complexity of the ALE calculation, which can be very high, but is still likely to be dependent on subjective probabilities.

Schetcher[123] claims that ALE does not specify how to forecast either loss events that will occur or reductions in rates that will result from adding safe guards.

8.5 Analysis and Discussion

In this section we analyze and discuss the findings from chapter 8.4 to obtain an understanding of the most prevalent causes of problems within ISRM.

One of the biggest problems identified in the existing ISRM literature is the lack of validation and verification of existing methods. This problem occurred in much of the visited literature and at different levels in the taxonomy. The qualitative methods and ALE/SLE were especially targets for this criticism. It is our opinion that being able to validate and verify if a method works would represent a huge leap in ISRM by putting a nail in the coffin for many of these discussions. In relation to this, although not mentioned in our taxonomy, we observed that none of the existing taxonomies we visited sorted ISRM methods on proven performance, such as measurable improvements in organizations. Related to the previous problem is the lack of empirical research and good data within IS. The reason for this is explained by Kotulic[97], and is still a major obstacle that need to be overcome to be able to make progress.

There must be tools available for IS professionals to be able to perform quantitative risk analysis; the literature points to a gap when it comes to explaining quantitative methods, referring to ALE/SLE and historical data as the quantitative approaches to ISRA. However, this presents a problem when there are apparent difficulties in calculating probabilities for ALE/SLE and little historical data available. There has been made attempts at solving the likelihood and probabilities problem by removing probabilities or making them optional, e.g. OCTAVE[20]. This introduces a new problem; without probabilities, we are no longer forecasting events. Can one conduct a meaningful risk analysis without addressing probability of an event occurring, and how does one address uncertainty without probabilities? Although few ISRM methods mention "cascading risks" and "common mode failures", "Failure mode and effect analysis" is a RA method that exists to address complex risks such as these. However, we do not know how popular this method is.

The misconception that ISRM is mainly an IT activity was a problem in 2001[36], and still is in 2013[71]. This knowledge gap seems therefore to be a prevalent cause for problems in ISRM. Viewing ISRM as a purely technical discipline, has among other things the potential of preventing human factors from being risk analyzed, disregarding intangible assets, and causing organizational disconnect in both managing risks and spending.

It is likely that many of the misconceptions about ISRM stem from the lack of a common IS and risk vocabulary. An example of this is the many definitions of the word *risk*. This

creates an obstacle for progression within IS, as professionals from different RM fields must first come to an agreement of what a risk is, before having a meaningful discussion on the topic.

There are several factors adding ambiguity to the ISRM process, and risk perception seem to be a prevalent problem. A large amount of literature points to people generally being bad at estimating risk: gender, age, race, emotional state, organizational rank, framing, etc... all affect how we perceive risk. It is unlikely that two people will rate a particular risk the same, and in addition to being susceptible to all of the above, subject experts tend to underestimate risk and show overconfidence in their own estimates. Related to both the risk vocabulary and perception is using subjective words to define risk likelihood and severity. The interpretation of the chance of a "high" probability risk occurring is likely to differ within an organization, compressing probability ranges to fit in risk matrices, and multiplication of results all add their own potential sources of error.

8.6 Conclusion

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

Article II - A Comparison between Business Process Management and Information Security Management

Gaute Wangen & Einar Snekkenes

A Comparison between Business Process Management and Information Security Management. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FEDCSIS), IEEE, 2014, 2, 901-910.

9.1 Abstract

Information Security Standards such as NIST SP 800-39 and ISO/IEC 27005:2011 are turning their scope towards business process security. And rightly so, as introducing an information security control into a business-processing environment is likely to affect business process flow, while redesigning a business process will most certainly have security implications. Hence, in this paper, we investigate the similarities and differences between Business Process Management (BPM) and Information Security Management (ISM), and explore the obstacles and opportunities for integrating the two concepts. We compare three levels of abstraction common for both approaches; top-level implementation strategies, organizational risk views & associated tasks, and domains. With some minor differences, the comparisons shows that there is a strong similarity in the implementation strategies, organizational views and tasks of both methods. The domain comparison shows that ISM maps to the BPM domains; however, some of the BPM domains have only limited support in ISM.

Keywords: Information Security, Information Security Risk Management, Business Process Management, BPM Methodology Framework, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST SP 800-39

9.2 Introduction

Information technology and systems play a crucial role by supporting the organization in achieving its goals and objectives. The main goal of information security (IS) is to secure the business against threats and ensure success in daily operations, and aid the businesses in reaching the desired level of reliability and productivity through ensuring integrity, availability and confidentiality[10]. We define the main profit of IS risk management (ISRM) as maximizing long term profit in the presence of faults, conflicting incentives and active adversaries.

Business Process management (BPM) is a discipline that combines knowledge from information technology and management sciences and centers on business processes[152]. It is used to represent business processes (BP) for analysis and improvement purposes[106, 51]. The main goals of BPM is to align the organization's business processes to the organization's mission, goals and objectives and improve efficiency to create a competitive advantage[70, 106].

Some of the existing information security frameworks mention risk management (RM) of business processes in some form, e.g. ISO/IEC 27005:2011 defines BPs as a primary asset[15], and NIST SP 800-39 suggests RM of Mission/Business Process as tier 2 in the multi tier organization-wide risk management model[103]. While the purpose of both IS management (ISM) and BPM is similar, to map and improve organizational performance in their own way, they remain two different disciplines that require two different sets of skill. In this paper, we investigate the similarities and differences between BPM and ISM, and explore the obstacles and opportunities for integrating the concepts of ISM and BPM. The BPM methodology framework[1] by BPTrends as described by Harmon[70] and Mahal[106] represents the main sources used to describe BPM, and we use the ISO/IEC 27000-series[13, 14, 15] and NIST SP 800-39[103] to describe ISM.

9.2.1 Problem Description

While it can be said that the scope of ISM is turning towards BPs security, BPM and ISM remain two different disciplines and are most of the time regarded as separate activities[83]. However, the disciplines mutually affect each other's objectives, e.g. re-engineering a BP will often have security implications, and introducing an information security control is likely to affect the BP flow. In addition, the impact of a materialized security risk will usually affect the business. A different set of skills is required to risk manage a BP than an IT-system; one requires knowledge of BPM methods, and the other technical insight in information security. In addition, there exists several types of BPs, ranging in abstraction level, from value chain at the very top of the organization, to work instruction & procedures[70, 106], see Fig. 9.1. People employed at different levels of the organization, perceive and worry about different risks[97], and focus on a variety of different goals in their work efforts[70]. The difference in abstraction makes it likely that one ISRM approach designed for a low level BP is not likely to be applicable for risk managing the higher abstractions, such as value chain or core processes. Hence, there is a need to make sure that IS and BPM activities are aligned. Very little has been published in terms of investigations regarding to what extent IS and BPM guidelines and methods are well aligned, overlapping or in conflict. The aim of this paper is to contribute towards the filling this gap.

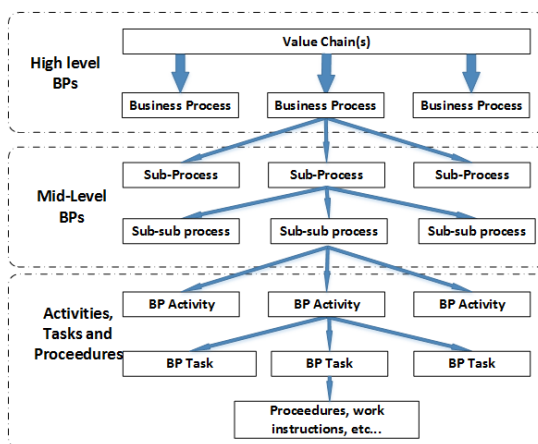


Figure 9.1: Example of a Business Process Hierarchy.

The remainder of this paper is structured as follows; In Sect. II, we present related work. In Sections III & IV we introduce relevant IS and BPM concepts used in this article. Sect. V introduces the research method. Sections VI, VII & VIII presents comparisons of

ISM and BPM and discussions of findings. The three areas of comparisons are Lifecycles, Organizational Views & corresponding tasks, and Domains. Conclusion and Future Work are given in Sect. IX.

9.3 Related Work

Much of the published research within combination of BPM and ISM focus on risk analysis of BPs; Milanovic et al.[110] presents a framework for modeling BP availability. The framework takes into account services, the underlying ICT-infrastructure and people, and has a special focus on dependencies between these layers. Jallow et.al. [84] present a framework for risk analyzing BPs, using modeling activities and Monte Carlo analysis for calculating risks and forecasts. Asnar and Massacci[25] takes the GRC management approach to information security, and presents a method for analyzing and designing security controls in an organizational setting using BPs. Zoet et.al.[174] introduces the different kinds of risk that affect a BP and establishes the relationship between operational risk, compliance risk, internal controls and business processes. Zoet et.al. also present an integrated framework for dealing with RM and compliance from a BP perspective. Taubenberger and Jurens[146] suggest to improve security processes by using BP models to move away from probabilities.

There also exists approaches for risk managing BPs; In 2000, Kokolakis et.al.[95] presented a paper discussing the use of BPM for IS. The authors argue that the asset-based approach of ISRM treats IS as an add-on feature aiming to minimize the overhead cost. The authors suggests that the combination of BPM and IS-SAD (information security analysis and design) techniques can be used for security re-engineering of a BP, and integration of IS. The authors presents an overview of existing BPM approaches and requirements they should support to be used in ISRM.

Jakoubi and Tjoa[83] introduce a reference model for considering information within the BPM and RM domains. The authors argue for a stronger interweaving between RM and BPM, and present an approach for reengineering business processes as risk-aware. Herrmann and Herrmann[72] introduces the MoSS BP (Modeling Security Semantics of Business Processes) frame, based on object-oriented process models. The authors introduce several security properties and correlations between security requirements and BP elements, together with the following general approach to risk managing business processes, the three first steps focus on identification of: (i) Business Processes and their actors. (ii) And valuation of assets and their security levels. (iii) Security requirements - and responding vulnerabilities and threats. While the two last steps address risk analysis and treatment: (iv) Assessment of risk. (v) Proposal, design and implementation of countermeasures.

AURUM[55] supports the NIST SP 800-30 standard[141], and is a framework for addressing IT risks which utilizes business processes for RM. AURUM prioritizes BPs based on importance, and derives the important assets from the BP. The method then continues to determine asset importance and conducts risk analysis based on Bayesian threat networks. Ozkan and Karabacak[115] suggests that process modeling can be used to ease the use of risk analysis methods and move the IS focus from hardware and software over to IT processes. The authors suggests using process modeling to model the activities of the information processing and to determine the scope of the risk analysis. The CERT Resilience Management Model v 1.0[45] (CERT RMM) is an approach for handling the challenge of operational resilience in day to day operations. The notion is that organizations deliver services that are supported by BPs' which are further supported by assets.

9.4 IT Governance, Information Security Risk & Management

Gregory[68] state that *"The purpose of IT governance is to align the IT-organization with the needs of the business"*. IT governance involves a series of activities to achieve this goal such

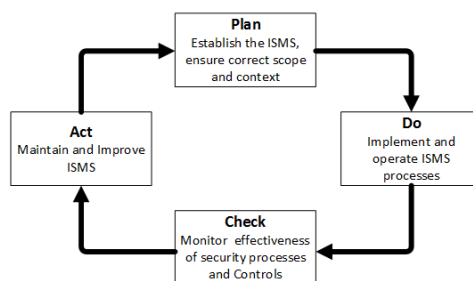


Figure 9.2: Plan Do Check Act-phases of ISMS implementation as described in ISO/IEC 27000:2009[10].

as creating IT-policy, internal prioritizing between e.g. mission, objectives and goals, program and project management[68]. It also includes the responsibility for managing risks appropriately, and verifying that resources are used responsibly[103].

9.4.1 Information Security Management (ISM)

Generally, the main goal of information security is to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity, availability (CIA) and non-repudiation[10]. Information can be present in many forms within the organization, it may be stored on a physical medium, be in the form of paper, or it can be an employee's knowledge and experience. Common for all these is that they are all valuable assets to an organization and their security needs assurance. One of the main components of ISM is to establish a security program, often referred to as an information security management system (ISMS). The ISMS is a collection of security related documents often with the company wide security policy as the main document. The purpose of the ISMS is to ensure CIA through management of the organization; by choosing and implementing the appropriate security measures and controls. These measures can be chosen from e.g. the ISO/IEC 27002 [14], which is a standard consisting of security measures and how to implement them. The ISMS can be implemented following a Plan-Do-Check-Act (PDCA) cycle of continuous improvement[10, 15], see Fig. 9.2. The security documentation of the ISMS is represented by a top-level security policy, generally founded in the organization's mission, vision, goals, values and objectives. Further represented by topic/issue-specific policies, standards, procedures and routines.

9.4.2 Information Security Risk Management (ISRM)

There exists several definitions of risk, ISO/IEC 31000:2009 [16] standard explains risk as *the effect of uncertainty on objectives*, and *Risk management* as a set of activities and methods applied in an organization to manage and control the many risks that can affect achievement of business goals. Hence, the main goal of ISRM is to maximize the long term profit, and optimally manage risks presented by potential failures, conflicting incentives and active adversaries.

A risk assessment is the *overall process of risk analysis and risk evaluation*[10], and risk analysis (RA) is the *systematic use of information to identify sources to estimate the risk*[10]. Risk evaluation is the *"process of comparing the estimated risk against given risk criteria to determine the significance of the risk"*[10].

ISO/IEC 27005:2011[15] is a standard specialized for ISRM and defines the formal process of managing risks as an iterative process of reviewing and monitoring risks, includ-

ing: context establishment, risk assessment, communication and treatment to obtain risk acceptance[15]. Risks for information systems are generally analyzed by using a probabilistic risk analysis (PRA) [141, 15], where impact to the organization (e.g. loss if a risk occurred) and the probability of the risk occurring is calculated. Probability calculation in ISRM has previously received criticism for relying too much on subjective estimates, and being too much like guesswork[35, 164, 68]. Risk evaluation uses the results from the analysis, and if the risk is found unacceptable, risk treatments are implemented, which consists of choosing a strategy and measures for controlling undesirable events.

9.4.3 Context Establishment for ISRM

The term "Context Establishment" is from the ISO/IEC Risk Management standard 27005[15], and defines both the external and the internal parameters that must be considered when managing risks. The internal context for ISRM will usually be a product of different factors, such as IT systems, stakeholders, governance, contractual relationships, culture, capabilities, business objectives, and others. Examples of relevant external factors for establishing context are external stakeholders, external environment, laws and regulations, and other factors that can affect the organizations objectives.

Many established ISRM methods center around assets, the *NIST Specification for Asset identification*[169] uses three main classes of information system related assets; (i) Persons, (ii) Organization, and (iii) Information Technology. In addition, it provides nine sub-classes of assets of Information technology. In contrast to this, ISO/IEC 27005:2011 uses two primary asset classes; (i) Business processes & activities" and (ii) Information, with supporting assets: (i) Hardware, (ii) Software, (iii) Network, (iv) Personell, (v) site, and (vi) organization's structure.

A control can exist as automatic or manual, an automatic control performs its function with little or no human interaction, and a manual control requires a human to operate it, and generally fall within three major categories[68]: (i) Physical - represents controls that are found in the physical world, such as fences, doors with locks, and laptop wires. (ii) Technical - represents controls that are implemented in the form of information systems, they are usually in a logical form, such as a firewall, antimalware, and computer access control. (iii) Administrative - represents controls in form of e.g. policies and procedures that forbid certain activities, such as the IS policy.

The 14 Control Clauses and security domains from ISO/IEC 27002:2011[14] and ISO/IEC 27001:2013[13] are:

1. Information Security Policy - Top level documented security objectives for the whole organization, determined by management.
2. Organization of Information Security - IS Roles and Responsibilities, and IS management in general.
3. Human Resources Security - IS requirements and controls for recruitment of staff, terms of employment, security awareness training and process for termination.
4. Asset Management - The management and application of hardware and software assets, and classifying and handling of information.
5. Access Control - Effective password, privilege and user management on operating systems, applications and within networks.
6. Cryptography - Controls for securing CIA of information using encryption.
7. Physical and Environmental Security - Securing the human and system environment, including entry controls, power and cabling security.
8. Operations Security - Ensure CIA of operations and facilities.

9. ARTICLE II - A COMPARISON BETWEEN BUSINESS PROCESS MANAGEMENT AND INFORMATION SECURITY MANAGEMENT

9. Communications Security - Key security aspects of managing systems securely, such as backups, antivirus, media and laptop security
10. System Acquisition, Development and Maintenance - Secure development of software and maintenance of systems to maintain ongoing security
11. Supplier Relationships - Protect the organization from security breaches caused by third parties.
12. Information Security Incident Management - The reporting, recording, management and review of security incidents.
13. Information security Aspects of Business Continuity Management - Determine requirements, plan and training for response in the event of disasters.
14. Compliance - Ensuring compliance with legal requirements, including IPR, computer misuse and privacy legislation.

9.5 Business Process Modelling and Management

A business process (BP) is a set of activities within an organization whose objective is to produce a desired result[18]. A process is, in short, "How work gets done"[106], and work is the "*exertion of effort directed to produce or accomplish something*"[51]. The purpose of modeling a BP is to describe the logical order and dependence, such that the practitioners can achieve a comprehensive understanding of the process[18]. A process generally has some sort input and transforms this into an output, e.g. a manufacturing process will take raw material as input, process this material, and output a product. We borrow the explanation from Mahal[106]: "a process is triggered by an event, governed by some rules using relevant knowledge, and executed through people using enabling technology and supporting infrastructure, such as facilities". A common abbreviation used to describe the components of a BP is IGOE - Inputs, guides, outputs and enablers[70, 106].

Besides from documenting processes, BPM can be used to facilitate large scale software developments to support BPs, BP analysis and improvement re-engineering[18]. The top-level representation of the BPM approach seen in Fig. 9.3.

9.5.1 The BPM Lifecycle

The BPM lifecycle represent the key activities in BPM. There is no uniform view of the number of BPM-LC phases[166]. Ko[93] state that there are many views of what steps the BPM life cycle actually consists of, and presents van der Aalst et.al.'s (2003)[153] view due to succinctness and relevance. Van der Aalst (2013)[152] has also published a newer review of the key activities in BPM after [93] was published. Wetzstein et.al.[166] present a general version of the BPM-LC. An analysis of the different lifecycle steps from [152, 153, 166, 94] show that they have the following steps in common:

1. Modeling and Design - Map/re-design or create a process model for analysis and/or enactment.
2. System Configuration & Implementation - Configure the system and implement the process model for enactment.
3. Enact/Execution - Deploy and execute the BP model using set configuration control and support concrete cases.
4. Monitor/Analyze - Analyze a process model studying the BP and/or event logs.
5. Manage/Diagnosis - Adjust/improve process, reallocate resources, manage large collections of BP models.

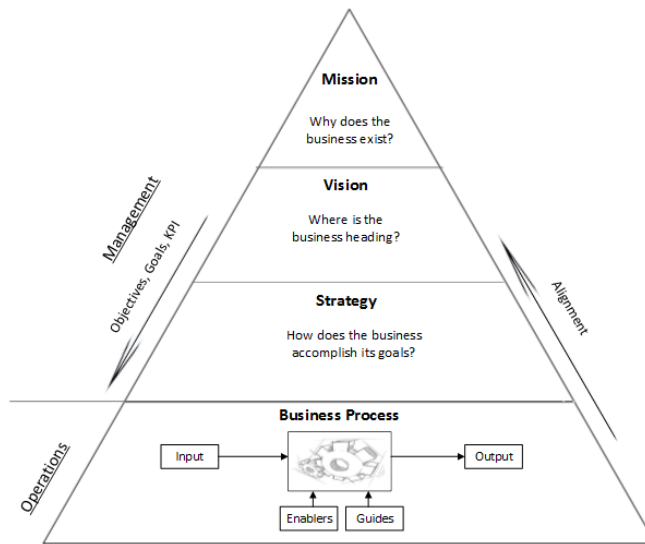


Figure 9.3: Connection between Mission, Vision, Strategy and Business Processes. *Based on Mahal[106]*

9.5.2 BPTrends Associates' BPM Methodology

The BPM Methodology Framework [1] is a best practices framework that provides a view of BPM sorted into three levels with associated steps. The framework recognizes the variety of goals at the different levels of the organization. The framework sorts the different levels into enterprise, process and implementation levels. The *Enterprise* level centers on corporate strategy, and focus on understanding and modeling BP architecture, defining performance measures, governance systems, aligning enterprise capabilities and prioritizing efforts. The main ongoing task consist of managing enterprise processes.

The *Process* level runs process improvement projects, where modeling, redesign and improvement of existing processes is in focus, taking processes from AS-IS to TO-BE. The main day-to-day tasks are BP execution and management.

The *Implementation* level focuses on designing human, software and information systems to implement BPs. It consists of various IT and HR methodologies that are used for maintaining resources and continuous improvement.

9.5.3 BP Domains

Fig. 9.4 illustrates the BP domains, and shows how the different aspects of business support the BP, which ultimately determines enterprise performance. The general purpose of a BP is to transform an input to a desired output. The enterprise delivers value to its stakeholders and customers, and enterprise performance can be described using a set of measurable goals and objectives. KPIs provide the mechanisms for measuring performance. Information, knowledge and insight is what fuels the BP. The BP execution transforms the information into knowledge which is applied to create solutions. The "Guides" manages and controls the input/output transformation[106]. Put in the information security language; Guides are generally about governance and controls. The "Enablers" are the reusable resources of an organization that support the BP in transformation of input to output[106]. We leave inputs and outputs out of scope in this comparison. An explanation of the BP

domains in the hexagon is as follows[106]: *Guides* provide governance, stakeholder expect-

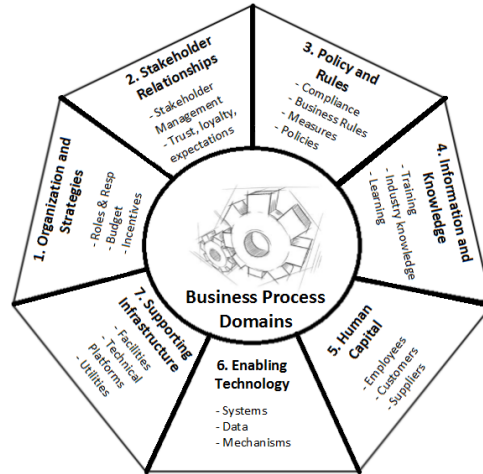


Figure 9.4: Illustration of Guides and Enablers that contribute to the BP. Based on [106, 40]

tations, direction, funding, rules and compliance restraints to the business process.

1. Organization and Strategies - Constitutes the organization's governance and its support structure. This domain covers consistent management, cohesive policies, processes, roles and responsibilities. It also includes organizational alignment and strategy development to achieve vision and deliver results.
2. Stakeholder Relationships - This domain constitutes both the external and internal stakeholders of the organization. It covers stakeholder management of expectations, trust and loyalty. The stakeholders are people who have vested in the success of the organization and can benefit from its performance.
3. Policy & Rules - Constitutes the business policies and rules of the organization, and are established to ensure compliance and mitigate risks through appropriate controls. The policies provide a decision-making framework at all levels of the organization.
4. Information and Knowledge - Encompasses training, learning and industry knowledge. *Defined as a guide in [106, 70].*

Enabler are the reusable resources of an organization that support the BP in transformation of input to output. Enablers provide execution capabilities for the BP.

5. Human Capital - Constitutes of the people who enables the process, namely employees, customers, and suppliers. For the employee it is about their competence, which encompasses of a combination of knowledge, skills and behavior. Capable people are essential to optimally executing a process.
6. Enabling Technology - Constitutes of the technology that enables the BP. Includes information technologies such as business applications, data stores, and mechanisms such as production lines, robots, and engineering equipment.
7. Supporting Infrastructure - Constitutes of production facilities, technical platforms, communications, utilities and energy, and other infrastructure. Can also be considered as the capital asset of the organization.

9.6 Method

The primary research method adopted in this work is analytical. This article uses theoretical comparisons and mapping of BPM and ISM, for each BP activity we look for a corresponding IS activity. Similarly, for each IS activity, we look for a corresponding BP activity. This process will identify the intersection of BP and IS as well as what activities that are missing if BP and IS "compliance" is desired.

Following Ko et.al.[94] we start at the very top of the abstraction levels, comparing the generic lifecycles of BPM and ISM. Staying at a high level of abstraction, we compare organization/risk views and corresponding tasks. Lastly, we do a domain comparison of the BPM and ISM.

9.7 A Comparison of ISM and BPM Lifecycles

The purpose of this section is to look for similarities and possibilities of integration between the top-level implementation strategies of the ISMS and BPM. We compare the high level steps of the plan-do-check-act (PDCA) lifecycle of the ISMS[13] and BPM lifecycle (BPM-LC) and look for common ground. Both cycles represent high-level views of the general activities of each approach. As there is no uniform view on the BPM-LC, we use the steps summarized in this article. We make the assumption that the ISMS lifecycle is compliant with the original PDCA-cycle, and compare the BPM-LC with the PDCA cycle as described by Moen and Norman[111].

Table 9.1: A Comparison of the generic PDCA steps and the BPM Lifecycle

<i>PDCA steps/ BPM Lifecycle</i>	Plan	Do	Check	Act
1. Modeling	X			
2. Implement/ Sys Config		X		
3. Enact/ Execution		X		
4. Analyze/ Monitor			X	
5. Manage/ Diagnosis				X

Table 9.1 shows that the generic BPM-lifecycle is loosely related to a PDCA notion of continuous improvement. A further comparison of the ISMS and BPM lifecycle approaches shows:

1. *Plan - Modelling*: The Plan-phase in ISMS is applied to establish context and scope the ISMS, together with planning for ISRM. In BPM, the steps in the modelling-phase maps existing BPs and plan/re-design BPs for enactment and analysis. Similar for both approaches is that they both establish the context and scope in this phase, the BPM uses BPs while IS uses e.g. an asset-based approach to establish organizational context. ISO/IEC 27005:2011[15] names BPs as one of two primary assets, which may open for a combined approach of BPM context establishment.
2. *Do - "System Configuration" & "Implementation and Enact/Execution"*: The steps in the Do-phase of the ISMS-lifecycle consists of implementing the processes associated with the ISMS. Usually in form of implementing risk treatment plans as a result of

the ISRM program.

The system configuration and implementation-phase in BPM implements designs by configuring process aware information systems and the underlying infrastructure. While the Enact/Execution phase executes and enacts the BP model. Both these BPM-phases correspond to the Do-phase in the PDCA cycle. Similar for both the ISMS and BPM lifecycles is that they both *implement* plans.

3. *Check - Analyze/Monitor*: This ISMS-phase monitors and reviews the effectiveness of implemented security process and residual risks. While the BPM-phase monitors and analyzes BPs for optimization. Both the IS and BPM lifecycles utilizes this phase for *monitoring and analysis* of the implemented processes.
4. *Act - Manage/Diagnosis*: The ISMS act-phase is mainly used to improve existing security processes based on analysis. The Manage and Diagnosis phase is utilized to adjust and improve BPs based on results from the previous lifecycle phase. This phase is also used to reallocate resources between BPs and manage large collections of BPs. Common for both lifecycles is implementing improvements based on analysis results from the previous phase.

We see from this comparison that the approaches are closely related; they are both founded on the PDCA principle, and the main tasks of each step is also similar.

9.8 A Comparison of Organizational Views

People employed at different levels of the organization both perceive and worry about different risks[97], which is also similar for the different concerns in the BPM hierarchy[70]. There is therefore a difference in what kind of information is needed to conduct tasks for both BPM and ISM at different levels of the organization. The purpose of this section is therefore to compare and map the organizational views and associated tasks presented in BPM and ISRM literature.

The BPM Methodology Framework represents a view of BPM sorted into levels including enterprise, process and implementation level, with recommended BPM steps per level (see [1, 106, 70]). NIST SP 800-39[103] presents three different tiers for ISRM views, the comparison between the organizational views can be seen in table 9.2.

The top-level comparison of the organizational views reveal a strong similarity. This is not surprising as one of NIST SP 800-39's main focus areas is securing BPs. Looking closer at the comparison we see a strong similarity in perspectives, tasks and responsibilities at each level:

- *Level 1* - We consider top management and organizational management to represent the same point of view. Both have a top-level management focus and are concerned with governance and strategy tasks. We use the BPM tasks as described by [1, 106] to compare the subtasks from ISRM. Since there is no standardized steps per level from NIST SP 800-39, we analyzed and summarized the following steps for level 1[103]: (i) Governance - assign roles and responsibilities to provide strategic direction, mission and objective achievement, risk management and resource usage, (ii) Strategic Alignment - of mission and business functions, (iii) Execution of Risk Management - frame, assess, respond to, and monitor risk (iv) Resource Allocation - of RM resources, (v) Measuring - monitoring and reporting RM metrics to ensure alignment, and (vi) Investment optimization - based on RM in support of organizational objectives.

The results from the comparison between ISRM and BPM level 1 sub-tasks can be seen in Fig. 9.5. The comparison show that the NIST RM function cover both *understanding the enterprise context* and *modelling enterprise processes* under Risk Framing, both activities necessary to conduct ISRM. However, the RM function only contributes to *Managing enterprise*

Table 9.2: A comparison of organizational views from the NIST SP 800-39[103] and BPM Methodology Framework[70, 106, 1]

Abstraction level	Category	Multitier Org -Wide RM	BPM Methodology Framework
Level 1	Perspective	Organizational	Enterprise
	Management	Top management	Organizational Management
	Main Tasks	Strategic risk management	Corporate Strategy in BPM, Supply chain
Level 2	Perspective	Mission/ Business Processes	Processes
	Management	Middle management	Process Management
	Main Tasks	RM of M/BP	Process Improvement
Level 3	Perspective	Information Systems	Implementation Level
	Management	Operations	Activity Management
	Main Tasks	Tactical Risk	Implementation of Information systems

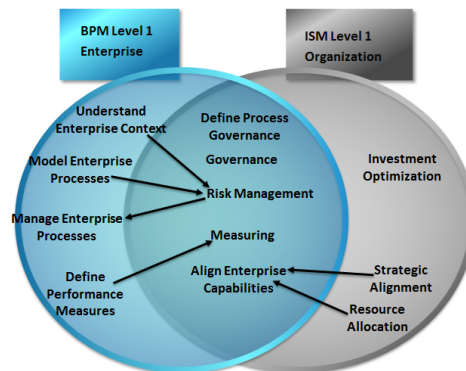


Figure 9.5: Illustration of common BPM & ISM Level 1 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.

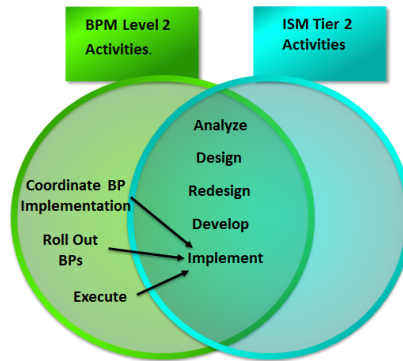


Figure 9.6: Illustration of common BPM & ISM Level 2 tasks. Arrows indicate that a task is part of an activity, and that conducting the individual task will not complete the activity.

processes which also includes activities such as establishing a BP services charter[106]. The same can be said for *Strategic alignment* of risk decisions, which is a part of completing *Aligning enterprise capabilities*, but does not complete the task. Our comparison show that there is no support for *Investment optimization* based on risk management at this level in BPM. Conducting resource allocation of RM resources will not complete any BPM tasks, but is a part of the *aligning enterprise capabilities* activity.

Comparing the other way, we see that there is no single ISRM Level 1 subtask to understand enterprise context and model enterprise context, but both are necessary steps in *execution of RM* task. While *defining performance measures* is a part of the ISRM activity *measuring*, we cannot say that completing the BPM activity also completes the ISRM task. However, managing enterprise processes also measures processes and allocates resources.

- *Level 2* - Middle management and Process management are descriptions of the same responsibilities and points of view, only differentiated by organizational structure (e.g. matrix based for process management, or traditional department-based organization for middle management)[70]. Both have a BP perspective, and are concerned with modeling, prioritizing and re-designing processes. Further comparison of level 2 subtasks is seen in Fig. 9.6, where we see that the Level 2 BPM activities resemble the BPM lifecycle. As there are no standard steps in NIST SP 800-39, we have summarized the following level 2 steps from [103] for developing Risk-aware BPs: (i) Design - Existing BP (AS-IS), (ii) Develop - secure BP (TO-BE), (iii) Implement - secure BP. The standard also suggests to develop Secure Enterprise Architecture (EA) as a Level 2 task, which comprises maximizing effectiveness of BPs and information resources. We regard this task as present in all the BP-ISRM steps, and therefore do not count it as a standalone task.

Our understanding of the NIST SP 800-39 tier two steps is that implementing a secure BP includes the BPM tasks "Coordination" (preparing for implementation), "Rolling out" and "Executing". Which means that all the BPM activities are supported in the ISRM approach. Comparing the other way shows that the "Analyze" and "Redesign" activities are covered by the ISRM steps, and that three remaining tasks together complete the ISRM "Implement" activity.

- *Level 3* - The information systems and implementation level perspective represents the operations and activity management point of view. The processes are found at the lower levels in the BPM hierarchy (see section 9.1), and represents where "the rubber meets the road"[106]. We consider this to represent the same management and perspective. Although

both BPM and ISRM share the operations view, they have slightly different concerns; IS is focused on securing information systems from tactical risks and managing controls, while BP is concerned with designing systems to implement with BPs.

As BPM employs several methodologies at this level, and the BPTrends associates' BPM Methodology framework does not extend to software and HR development[1], we have no standard tasks to compare to the ISRM. Mahal[106] mentions that one commonly used BPM method at this level is the software development lifecycle (SDLC). Risk managing the SDLC is also the main approach in NIST SP 800-39. Although concrete HR-strategies are not present in the NIST standard, it does discuss organizational culture and it does also discuss the topic of trust, which we can not see mentioned in the BPM literature.

9.9 A comparison of ISM and BPM domains

The main objective of this section is to compare the ISM and BPM domains to investigate if all control objectives can be integrated using BPM, and that all relevant aspects of BPM are covered in the control objectives. IS encompasses many fields related to information technology and systems, the ISO/IEC-standards in the 27000-series are industry standards and we use them as representatives of what must be covered to achieve IS (Notably ISO/IEC 27001 & 27002[13, 14]). Therefore, to compare BPM and ISM approaches we use the 14 security domains and controls from ISO/IEC 27002[14]. We mutually compare the IS domains to the domains of BPM defined by Burlton[40] and refined by Mahal[106] and Harmon[70].

9.9.1 Summary of Comparison, ISM and BPM

This section contains a summary of the integration results of IS into BPM. Table 9.3 shows a high level comparison of how the control clauses are supported by the BPM-domains.

The comparison of the ISM and BPM domains shows that we can integrate the security clauses and controls into the BPM domains of enablers and guides, and model them as BPs. An example is the implementation of the controls from the Information security incident management-security categories, illustrated in Fig. 9.7, which shows how the guides and enablers support the process.

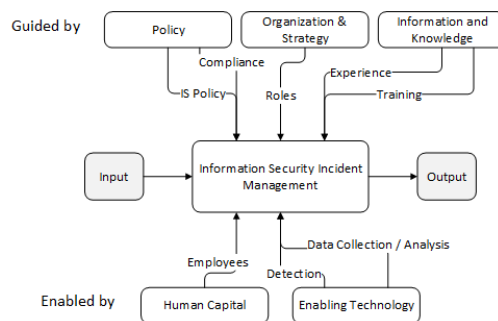


Figure 9.7: The illustration shows how the IS Incident Management control can be modelled within the BP domain.

One significant finding was that the domains of BPM does not directly consider internal or external attackers. This can in some cases be considered as a weakness of BPM as it concerns itself availability and integrity of BPs. RM is suggested as a supporting practice in development of the guides "Policy & Rules"[106]. The attacker might be considered as a part of general RM, but RM is such a wide discipline that it is likely to mean different things to different people[164].

9. ARTICLE II - A COMPARISON BETWEEN BUSINESS PROCESS MANAGEMENT AND INFORMATION SECURITY MANAGEMENT

Table 9.3: Summary of BPM-ISM and ISM-BPM comparison.

Legend: - "X" marks how the ISM domains are covered and can be implemented in the BPM domains.

- "0" marks which ISM domains support BPM domains and where.

Domains BPM	1.Organization and Strategy	2.Stakeholder Relationships	3.Policy and Rules	4.Information and Knowledge	5.Human Capital	6.Enabling Technology	7.Support Infrastructure
ISM Domains							
1.Information Security Policy	X	0	X	X	X		
2.Organization and IS	X	0	X	0	X	X	X
3.Human Resources Security	X		X	X	X	X	
4.Asset Management	X		X	X	X	X	X
5.Access Control			X	X	X	X	X
6.Cryptography			X	0	X	X	X
7.Physical and Environment Security			X	0	X	X	X
8.Operations security	X		X	X	X	X	X
9.Communications sec			X	X	X	X	X
10.System acquis, developm and mainte			X	X	X	X	X
11.Supplier relations		X (0)	X	X	X	X	X
12.IS incident man	X		X	X	X	X	X
13.IS aspect of BCM	X		X	X	X	X	X
14.Compliance			X	0	X	X	

BPM also presents a bit different view of assets; as the context, represented by BPs, is established before identifying the assets. In traditional ISRM, the situation is the other way around; first the asset that needs protection is identified, and then the context is modeled around the asset. Besides from knowledge, intangible assets are not reflected in the BPM domains.

Another result that can be seen from the comparison is that the enabler "Human Capital", which generally represents employees, are needed to implement and operate every ISM control domain. However, the comparison show that out of fourteen control domains, only four are related to the security of human capital.

9.9.2 Summary of Comparison, BPM and ISRM

This section contains a summary of the integration results of BPM into ISM. Our comparison shows that the controls in ISO/IEC 27002:2013 are properly scoped to address four of the seven BPM domains. The enabler-domains were all addressed, but there were issues when addressing three of the Guide-domains:

9.9.2.1 Organization and Strategies

ISO/IEC 27001, section 5.1 a) emphasizes IS policy's compatibility with the organizations strategic direction, however, it is not mentioned in one of ISO/IEC 27002's 114 controls that the IS policy should be aligned with business. We can make the assumption of alignment from clause control objective 5.1, which is to provide management direction and support for IS in accordance with business requirements and compliance. The control itself state that the policy should be defined and approved by management. This points to a difference in perspective between the two disciplines, where BPM hammers organizational alignment of BPs as one of its main mantras.

9.9.2.2 Stakeholder Relationships

Nurturing both internal and external stakeholder relationships is an essential component of BPM; stakeholder identification, steering expectation, ensuring trust and loyalty are essential to BPM success[106, 70, 88]. Section "6.1 Internal organization"[14] covers some stakeholder groups (without using that term), as authorities and "special interest groups" are both types of stakeholders. The suggested controls put emphasis on maintaining contact with these stakeholders. However, these external groups are per BPM definition not important stakeholders, ISO/IEC 27001:2013 address the stakeholder needs in section 4.2 *Understanding the needs and expectations of interested parties*, but we can not see this reflected in the control objectives. The ISMS-program risk failing if key stakeholders lose interest, several instances of failure due to not having sufficiently powerful allies is highlighted in [115]. Although not completely neglected by IS, there is a clear gap between how much emphasis BPM and ISRM put on stakeholder management.

9.9.2.3 Information and Knowledge

It is a given that information is covered by all of the security domains. In BPM, information is utilized as knowledge by employees to fuel BPs[106], and knowledge is generally possessed by employees. The "Return of Assets"- security control (8.1.4) briefly mentions knowledge; *In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization*. This reflects a preventive control at the *end* of an employment. Capturing knowledge presents difficulties, as the interviewer must know exactly what questions to ask and the subject must be cooperative and willing to communicate the information in a comprehensive way.

This brings up the question if an ISRM process can identify and protect critical knowledge. Knowledge is viewed as an intangible asset[147], but e.g. is not included in the asset overviews in [169] or [15]. However, loss of availability due to lack of knowledge is a plausible IS risk (e.g. during incident handling), combined with the importance of knowledge in BPM, makes it an important business area to secure. Depending on the skill of the analyst, knowledge runs the possibility of being overlooked by ISO/IEC 27005:2011 and asset-based approaches.

9.10 Conclusion

We have shown in this article that both the top-level BPM and ISM approaches are based on a Deming-cycle (PDCA) of continuous improvement, and that the main tasks of each step are similar.

We have shown that there is a strong similarity between the BPM Methodology framework and the ISRM standard NIST SP 800-39, as both approaches uses similar organizational views, only applying different names. We have also shown that the tasks and goals of each level are similar, with some key differences: the tier/level 1 ISRM approach does not in-

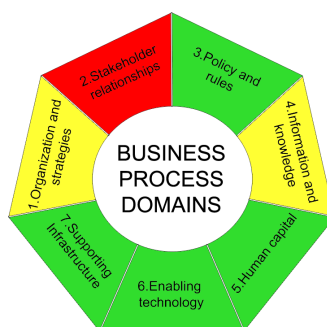


Figure 9.8: Heatmap indicating how well ISM covers the BPM domains, green signals no issues, red signals significant issues.

clude an activity for managing enterprise processes, and BPM does not include risk based investment optimization and trust-issues.

When comparing BPM and ISM domains we found that the ISM tasks can be supported by BPM, but that BPM does not include the concept of internal or external attackers. Further we found that ISO/IEC 27001/2 standards emphasized, but not controlled that the IS policy was aligned with business requirements. We also found a large gap between how much emphasis ISM and BPM put on stakeholders. Where BPM have fully adopted the principles of stakeholder management and recognized its importance, there is no real approach adopted in ISM to address stakeholders. We also found that the need for securing knowledge possibly is underestimated in ISM.

9.10.1 Future Work

As our findings are theoretical, we suggest further validation of the results from this article. This article has also shown that there is some common ground between BPM and ISM, and this warrants further investigation to determine if a joint approach is feasible. This work has revealed the potential for further research concerning stakeholder management in information security.

Acknowledgements

The authors of this paper thanks the anonymous reviewers for their valuable comments and suggestions. The PHD-student is sponsored by COINS Research School for IS.

Article III - An Initial Insight Into InfoSec Risk Management Practices

Gaute Wangen

An Initial Insight Into InfoSec Risk Management Practices. Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2015 - Ålesund, Open Journal Systems, 2015, 2015.

10.1 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

10.2 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 [164], the literature is scarce regarding the current ISRM industry practices. There are several known theoretical problems in ISRM[164], 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 problems outlined in previous work [164] reflect problems experienced in the industry?". Due to the width of the field, we have narrowed the scope of this research to investigate

¹*This version has been changed from the published version, see the Erratum at the end of the paper for changes.*

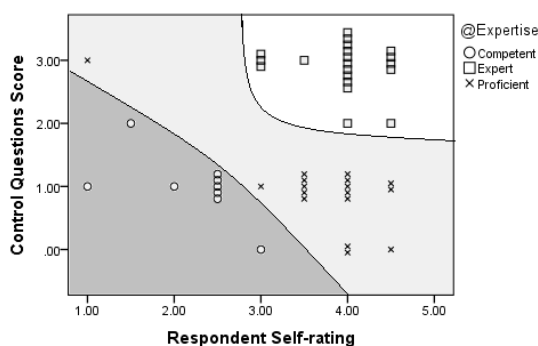


Figure 10.1: How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)

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[36]. While ISRM is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve acceptance[15]. The issues investigated in this paper primarily builds on the findings of the survey paper "A Taxonomy of Challenges in ISRM" [164], 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.

10.3 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 [164]. 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.

10.3.1 Data Collection - Online Questionnaire

One of the most prominent problems in InfoSec studies is getting in touch with the target group and acquiring respondents [97]. 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 [97]. 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 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 10.1. 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. 10.1.

We designed the questionnaire in Google Forms according to the procedure for developing better measures [50]. 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 10.1: Groups and Forums where the questionnaire was posted

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

10.3.2 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 [154]:

For *Descriptive analysis* we have considered distributions including range and standard deviation. On continuous type questions, we applied the median as the primary measure of central tendency. 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 re-

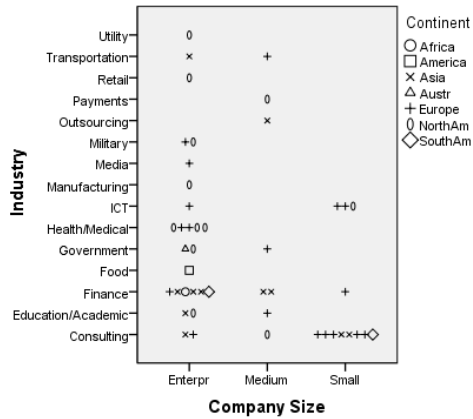


Figure 10.2: Respondent demographics, based on company size (x-axis), industry (Y-axis) and Continent.

spondent to write a comment and offer further qualitative insight on an issue, where the most valuable comments are a part of this paper.

10.4 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.

10.4.1 Respondents and Demography

The questionnaire was deployed on specialized InfoSec risk forums on LinkedIN.com, Table 10.1, where we received 46 accepted answers. See Table 10.2 for the classification of respondent expertise and work type (technical or administrative). While Fig. 10.2 displays respondent demographics categorized on company size, industry, and geographical affiliation.

10.4.2 Risk Definitions

We find one of the issues with the ISRM vocabulary in the many definitions of what an InfoSec risk is [164]. 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 10.3. 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

Table 10.2: Classification of Respondents, total 46.

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

Experts reported that he agreed with the ISO/IEC 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".

Table 10.3: 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)
$((\text{Vulnerability} * \text{Threat}) / \text{Counter Measure}) * \text{Asset Value at Risk}$	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%	

10.4.3 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 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, see the total median in Table 10.4. The Table also shows a noticeable difference in responsibility from company sizes.

Table 10.4: Answers to "Our ISRM program is ran by our IT department" sorted by company size.

@CompanySize	N	Minimum	Maximum	Range	Median	Grouped Median	Variance
Enterpr	26	1	6	5	4,50	4,25	3,122
Medium	8	1	5	4	3,50	3,33	2,214
Small	12	1	6	5	2,00	2,00	3,356
Total	46	1	6	5	3,50	3,50	3,177

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 median = 9, Range = 5, and Variance = 1,7. We also asked if the participants thought the cost of developing and implementing the ISRM program superseded the benefits the respondents were more divided, median = 4, range = 9, and variance 7,2. 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 10.6. All the participants to various degrees based their choice of ISRM approach on recommendations from Experts or others, showing no notable 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 median = 4, range = 5 and variance = 2,1 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 10.5, the results display a an observable difference between the Expertise groups, notably the Expert and Competent group. Indicating that the Expert group is more likely to apply industry standards for their ISRM development.

Table 10.5: Differences in application of industry standards for ISRM program development

@Expertise	N	Minimum	Maximum	Range	Median	Grouped Median	Variance
Competent	9	2	6	4	4,00	4,00	1,750
Expert	20	3	6	3	6,00	5,36	1,187
Proficient	17	2	6	4	5,00	4,88	1,596
Total	46	2	6	4	5,00	5,00	1,564

The ISRM literature lists several claims regarding the scope of ISRM being too technical [164]. 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 [164]. 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 10.6.

10.4.3.1 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.

10.4.3.2 Comments on measuring efficiency of the program.

Measuring security is one of the key problems in the InfoSec community [164] 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

Table 10.6: 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).

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 10.7: Perceived contributions of the ISRM program to different areas

	N	Minimum	Maximum	Range	Median	Grouped Median	Variance
29_1 Asset protection	46	2	6	4	5,00	5,00	1,374
29_2 Compliance with laws and regulations	46	2	6	4	5,00	5,06	1,360
29_3 Improved Corporate competitiveness	46	1	6	5	4,00	3,68	2,199
29_4 Increase Customer base	46	1	6	5	3,00	3,10	2,399
29_5 Increased Production	46	1	6	5	3,00	3,38	1,932
29_6 Managing Security Investments	46	1	6	5	4,00	4,17	1,865
29_7 Mapping ICT Business Criticality	46	2	6	4	5,00	4,43	1,438
29_8 Reliable and Secure Operations	46	2	6	4	5,00	5,20	1,088
29_9 Safeguarding Systems	46	2	6	4	5,00	5,21	1,133
29_10 Safeguarding Employees	46	1	6	5	4,00	4,16	2,188
29_11 Security Management	46	2	6	4	5,00	5,00	1,347
29_12 Threat Intelligence	46	2	6	4	4,00	4,30	1,807

10.4.4 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 10.7 for the descriptive results. Notable findings are listed in Table 10.8. We found an observable 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 finding 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. 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. There was also difference in perceptions from the different expert groups, both Proficient and Expert respondents had a median of 4 while the competent group had 5.

Table 10.8: Observable differences between categories from ISRM contributions

	Class	N	Min	Max	Range	Median	Gr. Med.	Var.
29_4 Increase Customer base								
CompanySize	Enterpr	26	1	5	4	2,50	2,55	1,614
	Medium	8	2	6	4	3,00	3,67	1,929
	Small	12	1	6	5	4,00	4,00	3,091
	Total	46	1	6	5	3,00	3,10	2,399
29_5 Increased Production								
CompanySize	Enterpr	26	1	5	4	3,00	3,13	1,440
	Medium	8	2	6	4	3,50	3,75	1,839
	Small	12	1	6	5	4,00	3,83	2,629
	Total	46	1	6	5	3,00	3,38	1,932
29_7 Mapping ICT Business Criticality								
CompanySize	Enterpr	26	2	6	4	4,00	3,88	1,158
	Medium	8	3	6	3	5,00	4,83	,786
	Small	12	2	6	4	5,50	5,33	1,818
	Total	46	2	6	4	5,00	4,43	1,438
29_6 Managing Security Investments								
Expertise	Expert	20	1	6	5	4,00	3,91	1,463
	Proficient	17	1	6	5	4,00	4,25	2,684
	Competent	9	2	6	4	5,00	4,50	1,500
	Total	46	1	6	5	4,00	4,17	1,865
WorkType	Tech	17	2	6	4	5,00	4,73	1,257
	Admin	29	1	6	5	4,00	3,75	1,993
	Total	46	1	6	5	4,00	4,17	1,865

10.4.4.1 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, bal-

ancing investments, and improving decision-making. (iv) Eight listed maintenance of *trust and reputation* in terms of internally, partners, and competitiveness as a primary reason.

10.4.5 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."*

10.5 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 section 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 10.3). The preferred ISO/IEC 27005:2005 risk definition is built on the classic $Risk = Probability \times Consequence$ 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 [162], 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 10.6). 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 [36]. 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 10.6 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 [164]. 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 10.6). 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 10.7 & 10.8). 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 notable 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 the 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 certifica-

tions 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 [164]. 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.

10.5.1 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.

10.6 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 $R=P \times C$ 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.

<i>Section</i>	<i>Original Text</i>	<i>Replaced</i>
2. Research Method - Analysis	See full paper in Appendix for the original method description.	New method description for "Analysis". See paper.
Whole paper - Changed wording	Changed word "Significant" when discussing statistical analysis (not including correlations). Word "Significant" implies statistical significance, since our updated method does not allow for significance tests, we changed this word throughout the text to avoid misunderstandings.	Changed to "observable" and "notable"
3. Results - ISRM Perceptions, Scope, and development.	<i>Table 4 - Had measurements of Mean, Standard Deviation, Std. Error, 95% CI, Min, Max, and ANOVA</i>	Table 4 - Changed to include Min, max, range, median, grouped median, range
	<i>Text connected to Table 4.</i>	<i>Added:</i> "... the total median in Table 4. The Table also shows a noticeable difference in responsibility from company sizes."
	Important they considered the ISRM process to be in achieving InfoSec - "The results showed a mean value = 8.6 and Std.Dev. = 1.3."	"The results showed a median = 9, Range = 5, and Variance = ~1,7."
	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."	"median = 4, range = 9, and variance 7,2."
	agreed entirely with this statement, "with a mean = 3.65"	agreed entirely with this statement, with a median = 4, range = 5 and variance = 2,1
	<i>Table 5 Had measurements of Mean, Standard Deviation, Std. Error, 95% CI, Min, Max, and ANOVA</i>	Table 4 - Changed to include Min, max, range, median, grouped median, range
	"... 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."	... the results display a an observable difference between the Expertise groups, notably the Expert and Competent group. Indicating that the Expert group is more likely to apply industry standards for their ISRM development.
3. Results - ISRM Contributions of the ISRM program	<i>Table 7 - Had measurements of Mean and Std. Dev.</i>	Table 7 - Changed to Median, grouped median, and Variance.
	"Statistically significant findings are listed in Table 7. We found a significant difference.. "	Notable findings are listed in Table 7. We found an observable difference...
	"Another significant finding (within 90% confidence) was regarding the \textit{Increased Production} statement,"	Another finding was regarding the \textit{Increased Production} statement,
	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.	There was also difference in perceptions from the different expert groups, both Proficient and Expert respondents had a median of 4 while the competent group had 5.

Figure 10.3: Overview of Erratum

10.7 Erratum

This article has been significantly changed from the published version in Proceeding of Norwegian Information Security Conference [157]. The reason for this was that the original paper was published with an inappropriate choice of statistical method data analysis. The original paper had made use of inappropriate measurements of central tendency; The mean value and significance tests were incorrect since there are was no defined interval in the Likert-type scale used for data collection. All the listed changes in Table 10.3 are changes to the statistical analysis and measurement of central tendency.

10. ARTICLE III - AN INITIAL INSIGHT INTO INFOSEC RISK MANAGEMENT PRACTICES

Article IV - An Initial Insight Into Information Security Risk Assessment Practices

Gaute Wangen

An initial insight into Information Security Risk Assessment practices Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, IEEE, 2016, 8, 999-1008.

11.1 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 we 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.

11.2 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 [11]. Best practice InfoSec is highly dependent on well-functioning InfoSec risk management (ISRM) processes[36]. While ISRM is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve acceptance[15].

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 [164], the literature is scarce regarding the current ISRA industry practices. There are several known theoretical problems in ISRA[164, 58], 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 [157] 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 ([164]) reflect problems experienced in the industry?". The scope of this article covers the ISRA process, including risk identification, estimation, evaluation, and risk treatment practices [15], 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.

11.2.1 Related work

This work primarily builds on previous work conducted on the topic of research problems in ISRM/ISRA. Both Wangen and Snekenes [164] and Fenz et al. [58] 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 [157].

11.3 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 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.

11.3.1 Data Collection, Sample, and Measurement

In their study, Kotulic and Clark [97] 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 [97]. 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

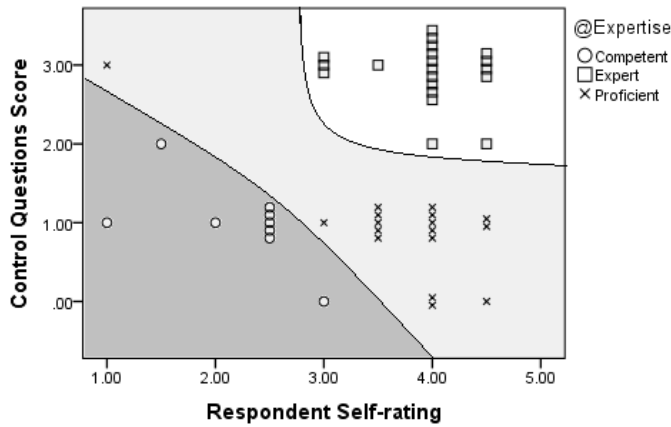


Figure 11.1: How respondents ranked themselves (x-axis) and how they were rated in the survey (Y-axis)

particular forums, Table 11.1. 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. 11.1.

We designed the questionnaire in Google Forms according to the procedure for developing better measures [50]. 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. 11.1, 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 11.1: Groups and Forums where the questionnaire was posted

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

11.3.2 Demographics

We received 46 accepted answers, See Table 11.2 for the classification of respondent expertise and work type (technical or administrative). While Fig. 11.2 displays respondent

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

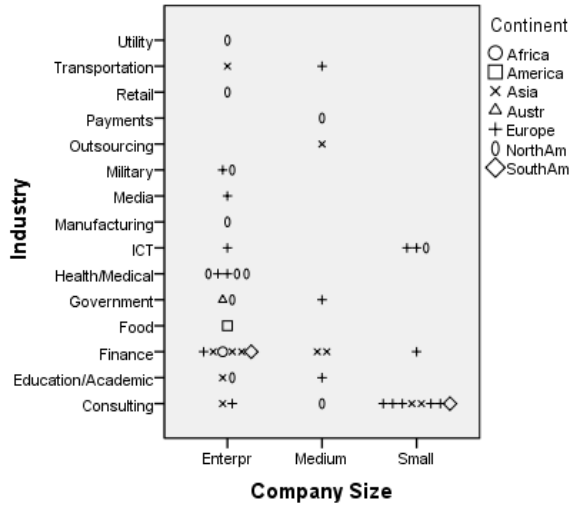


Figure 11.2: Respondent demographics, based on company size (x-axis), industry (Y-axis) and Continent.

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 11.2: Classification of Respondents, total 46.

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

11.3.3 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.

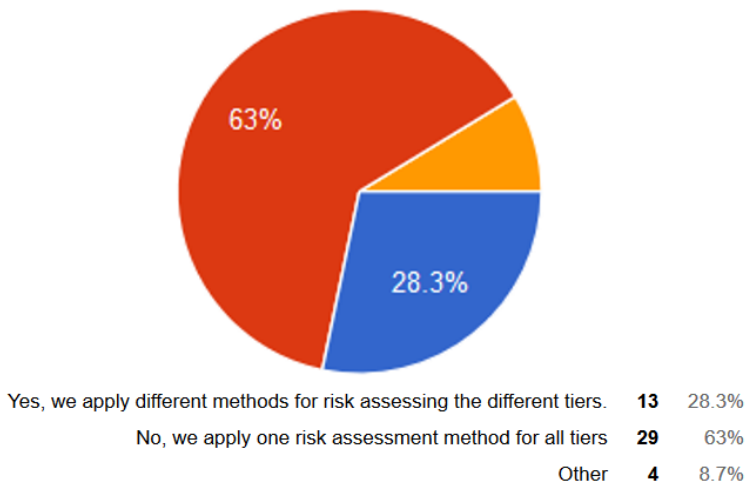


Figure 11.3: ISRA practices on different organizational tiers

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.

11.4 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.

11.4.1 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 [103]). 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. 11.3. 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."*

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"),*

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

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.

11.4.2 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 the 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 11.3 holds an overview of who attends ISRAs in the respondents organizations. The alternatives were "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 11.4.

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 11.4. 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 11.3, 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."*

11.4.3 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 11.5. 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 from its practitioners.

There were three noticeable differences between the expertise categories, the difference in

¹Edited 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."*

Table 11.3: 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 11.4: 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

view between experts and the two other groups on the importance of software, threat intelligence, and ISRA methods, Table 11.6. 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.

11.5 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

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

Table 11.5: 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 11.6: 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

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."

11.5.1 Views on Information Assets

Asset evaluation is one of the key challenges in ISRA [164, 57]. 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 [164]. Figure 11.4 shows the distribution of answers and Table 11.7 displays descriptive statistics, typical of these results is a high variability in the answers.

With regards to Statement 1 (Table 11.7), 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) [164].

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 11.4, 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 11.8, showing the Experts being less satisfied with the available asset value estimation methods. Three admin experts also com-

mented 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 [173] 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 organization's business processes. Statements 3 and 4 (Table 11.7 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 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 11.8.

Table 11.7: 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

11.5.2 Views on common Risk Analysis issues

The qualitative versus quantitative risk assessment is a well-known debate in ISRA [164], 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 [164]. With the described issue at its core, we asked the participants to rank several statements regarding ISRA practices, Table 11.9 holds the statements with results and the distributions are in Table 11.10. The results were diverse regarding all the statements, with the lowest median at 3 and highest at 5. In the following text, we ana-

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

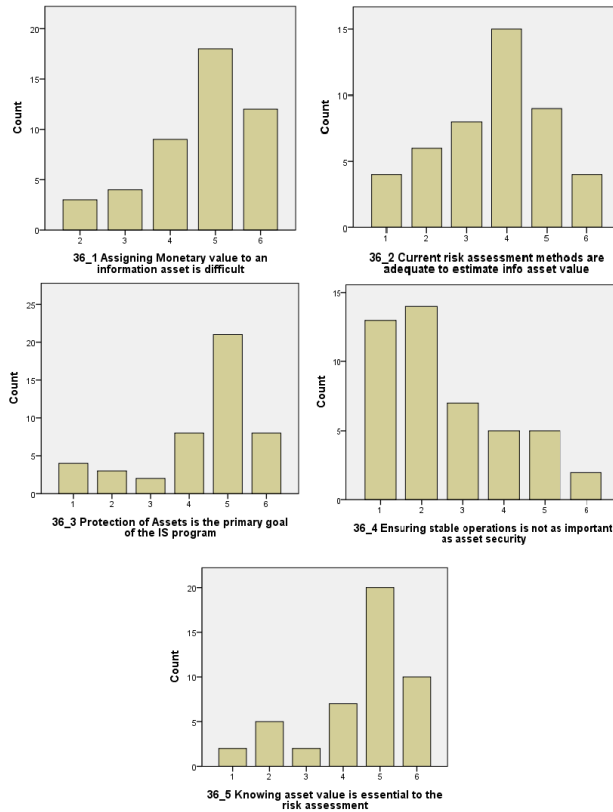


Figure 11.4: Statements and rankings regarding Assets (Scale 1 - *Strongly disagree* to 6 - *Strongly agree*)

Table 11.8: Statistically significant and notable differences between expertise categories on assets

Asset Scenario	Category	N	Mean	Std. Dev.	95% CI		Min	Max	ANOVA, sig
					Lower Bound	Upper Bound			
2.	Competent	9	4,44	0,882	3,77	5,12	3	6	.031
	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	
		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	

Table 11.9: Descriptive statistics of ISRA statements. (1 - Strongly Disagree, 6 - Strongly Agree)

	N	Min	Max	Mean	Variance	Median	Skewness	Range
S1.Our ISRA Methods are mainly Qualitative	46	2	6	4,41	1,537	5	-,414	4
S2.Our ISRA Methods are mainly Quantitative/Statistical	46	1	6	3,26	2,597	3	,254	5
S3.It is easy to use the ISRA results to predict the monetary cost of an incident	46	1	6	3,13	2,338	3	,161	5
S4.Our ISRA 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 ISRA 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 11.10: Distribution of answers (x-axis) regarding ISRA statements (y-axis). Statement numbers correlate with descriptions in Table 11.9. (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%)

lyze 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 11.11, 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 ISRA 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 11.11 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 11.12.

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

ISRA 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 ISRA 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 [104], the Narrative Fallacy [144]), and involve a high degree of guesswork (see [164]). S4, regarding ISRA 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 11.11), where small and medium companies seem more reliant on expert predictions than the enterprise-sized organizations.

Regarding S5, asks if spending resources on quantitative ISRA 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 11.11). 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 [164] 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 [164], S7 and S8 connects to this issue. S7 addresses views on the adequacy of mathematical ISRA 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 [162] and may be one of the causes.

Both S10 and S11 are connected to unforeseen incidents and causes, both related to Black Swan Risks [144] 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 [162, 164, 57], where the factors that limit the forecasting are, for example, complexity, interconnectivity, and active adversaries. These factors do not apply for all InfoSec risks [162] and there is utility in obtaining statistical distributions of InfoSec risks [162]. 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 11.11: Notable difference between categories (Full statements correspond to numbers in Table 11.9)

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

11.5.3 Correlations between statements

Several of the statements have strongly correlating results, Table 11.12. 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 11.7; *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 any-*

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

thing 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 11.12: Correlations between ISRAn statements. (Full statements correspond to numbers in Table 11.9)

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

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

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

11.5.4 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 11.13 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 [33, 144, 145]), 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 [144] and ALARP (As Low As Reasonably Practicable) [33] 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 11.13: 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

11.5.5 Cost-effectiveness of ISRA methods

As a follow up, we asked the participants which ISRA 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 (pen-tests), 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 [33]. *Bowtie* are used for both risk analysis, visualization and communication.

11.5.6 What is the most important task of the ISRA?

There several tasks that are common when conducting an ISRA [161], we gathered the common denominators and asked the participants to rate them according to their importance, 1 - Not important to 6 - Very important. Table 11.14 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

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK ASSESSMENT PRACTICES

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 11.14: 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

11.6 Choosing Risk Treatment Strategies

Jaquith [85] claims that for most people, risk management really means risk identification, although these phases are clearly defined in the ISO/IEC vocabulary [11]. Applying ISO/IEC 27005:2011 [15] 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 11.15 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 11.15: 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.[36] 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 11.16 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 11.16: 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. 11.5 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.

11.7 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.

11.7.1 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

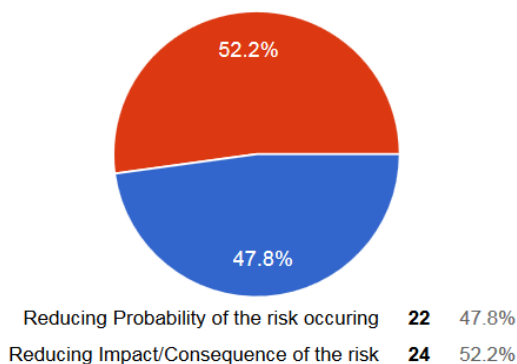


Figure 11.5: Results from opting to reduce either probability or consequence

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.

11.7.2 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 ISRA approaches are qualitative. While those who described their work as more technical were more likely to describe their ISRA 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.

11. ARTICLE IV - AN INITIAL INSIGHT INTO INFORMATION SECURITY RISK
ASSESSMENT PRACTICES

Article V - A framework for estimating information security risk assessment method completeness - Core Unified Risk Framework, CURF

Gaute Wangen, Christoffer Hallstensen, & Einar Snekkenes
Framework for estimating information security risk assessment method completeness - Core Unified Risk Framework. [Submitted Manuscript 2015], 2017.

12.1 Abstract

In general, an Information Security Risk Assessment (ISRA) method produce probabilistic risk estimates, where risk is the product of the probability of a given occurrence and the consequence of the event for the given organization. ISRA practices vary from industries and discipline, resulting in various approaches and methods for risk assessment. There exist several methods for comparing ISRA methods, but these are scoped to compare the content of the methods to a predefined set of criteria, rather than process activities to be carried out and the issues the method is designed to address. It is the lack of an all-inclusive, comprehensive comparison that motivates this work. This paper proposes the Core Unified Risk Framework (CURF) as an approach to compare different methods. We developed CURF as an all-inclusive (Unified) ISRA model, growing it organically by adding new issues and tasks from each reviewed method. If a task or issue was present in surveyed ISRA method, but not in CURF, it was appended to the model, thus, obtaining a measure of completeness for the studied methods. The scope of this work is primarily functional approaches risk assessment procedures, which are the formal ISRA methods that focus on assessments of assets, threats, and protections, often with measures of probability and consequence. This study does not address aspects beyond risk identification, estimation, and evaluation. This approach allowed for a detailed qualitative comparison of processes and activities in each method and provided a measure of completeness. We found the "ISO/IEC 27005 Information Security Risk Management" to be the most complete approach at present, with the Factor Analysis of Information Risk (FAIR) as the most complete risk estimation method. In addition, we also discovered several gaps in the surveyed methods.

Keywords: Information Security, Risk Assessment, Methodology, Completeness

12.2 Introduction

Information security (InfoSec) risk comes from applying technology to information [36], where the risks revolve around securing the confidentiality, integrity, and availability of information. InfoSec risk management (ISRM) is the process of managing these risks, to be more specific; the practice of continuously identifying, reviewing, treating and monitoring risks to achieve risk acceptance, illustrated in Fig. 12.1. A baseline level of security can be achieved through compliance with current law and legislation, but best practice InfoSec is

highly dependent on well-functioning ISRM processes[36], which requires a tailored program to suit the risk taking of the organization. Typically, risks for information systems are analyzed using a probabilistic risk analysis, where risk is a measure of the probability of occurrence and the consequence for the organization (e.g. financial loss if a risk occurred). There are many different definitions of risk [29] and many different risk assessment methods [2, 38, 142, 126, 44, 127], InfoSec risk assessment (ISRA) practices vary between industries, disciplines, and even within the same organization, which has brought a variety of ISRA methods and risk definitions. This article covers the risk assessment process, including risk identification, estimation, and evaluation, and compares the completeness of eleven surveyed ISRA methods. The main difference between risk assessment and analysis is, according to ISO/IEC 27000:2016 [12], that the latter does not include the risk evaluation. Further, we develop a framework for comparing ISRA methods on their completeness. We demonstrate the utility of the framework by applying it to a collection of risk assessment methods, identifying several limitations and weaknesses of existing risk analysis, of which several were previously not well known. For example, besides the FAIR approach [62] there are few detailed approaches to obtaining quantitative estimates regarding the probability of occurrence. All of the surveyed methods include an approach for qualitatively describing risk impact, while only three of the eleven methods guide how to quantify loss estimates. Asset identification and evaluation are two of the most common risk identification activities, but very few methods include the business process in the asset identification. Although business processes are defined as one of two primary assets in ISO/IEC 27005:2011 [15]. Our results show that risk concepts, such as opportunity cost, cloud risk, incentive calculations, and privacy risk estimations have a small penetration in the surveyed methods. Also, none of the studied methods discuss the Black Swan concept proposed by Taleb [144], or fully adopted the *Knowledge*-metric of qualitative risk assessments as suggested by Aven and Renn [32].

Note that our comparison framework is restricted to risk assessment and that we apply the framework to the risk analysis and evaluation part of some risk management methods. Thus, a comparison of non-risk analysis elements of risk management methods is outside the scope of our work.

Using the terminology established by Campbell and Stamp [44]; the extent of this work is primary *functional* approaches [44], which are the formal ISRA methods that focus on assessments of threats and protections, often with measures of probability and consequence. As opposed to *temporal* approaches that tests components of actual attacks, such as penetration tests and red teams. While *comparative* methods compare systems to best practices and establishes security baselines. The scope of this article is limited to the InfoSec risk approaches. We have not evaluated accompanying software tools for each method in Core Unified Risk Framework (CURF). Some methods, such as FAIR and CRAMM [170] come with software that expands aspects of the approach.

The remainder of the paper is organized as follows, Section 12.3 provides general background information on the eleven surveyed ISRA methods. In section 12.4, we present the design science research approach applied to develop CURF. Further, In section 12.5, we implement the framework on popular ISRA methods and show the results. Further, we discuss the completeness of each surveyed method and limitations of current approaches in sections 12.6 and 12.7. Lastly, we establish the relationship to other literature in section 12.8, and conclude in section 12.9 together with proposals for future work.

12.3 Reviewed Methods

In this paper, we have reviewed nine well documented ISRA methods which all have in common that they have been specifically developed to address InfoSec risk and are well-documented. In addition, CURF contains one review of both a Privacy and a Cloud risk assessment method. The following is a summary of the eleven methods:

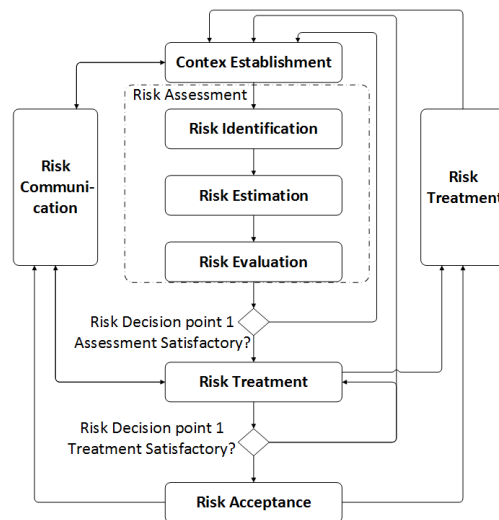


Figure 12.1: The ISO/IEC 27005:2011 ISRM process, the *Risk Assessment* activities mark the scope of this paper.

CIRA is a risk assessment method developed primarily by Rajbhandari [117] and Snekenes [134]. CIRA frames risk regarding conflicting incentives between stakeholders, such information asymmetry situations and moral hazard situations. It focuses on the stakeholders, their actions and perceived outcomes of these actions.

CORAS is a UML (Unified Modeling Language) model-based security risk analysis method developed for InfoSec [105, 52]. CORAS defines a UML-language for security concepts such as threat, asset, vulnerability, and scenario, which is applied to model incidents.

The CCTA Risk Analysis and Management Method (CRAMM v.5) is a qualitative ISRA method [170]. CRAMM is specifically built around the supporting tool with the same name and refers to descriptions provided in the repositories and databases present in the tool.

FAIR (Factor Analysis of Information Risks) is a risk assessment method, and one of the few primarily quantitative ISRA approaches [87, 62]. FAIR breaks risks down into twelve specific factors, which contains four well-defined factors for the loss and probability calculations. FAIR includes ways to measure the different factors and to derive quantitative analysis results.

The Norwegian National Security Authority Risk and Vulnerability Assessment (NSM ROS) [113] approach was designed for aiding organizations in their effort to become compliant with the Norwegian Security Act.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro methodology is the most recent method of the OCTAVE-family [46], aimed at being less extensive than the previous installments of OCTAVE. It is a lightweight version of the original OCTAVE and was designed as a streamlined process to facilitate risk assessments without the need for InfoSec experts and still produce robust results [46](P.4).

The ISO/IEC 27005:2011 - Information technology, Security techniques, Information Security Risk Management [15] details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood.

The current installment of the NIST SP 800-30 - Guide for Conducting Risk Assessments is at revision one [37], and was developed to further statutory responsibilities under the Federal Information Security Management Act. NIST SP 800-30 rev. one was designed for

larger and complex organizations. The purpose of the publication was to produce a unified information security framework for the U.S. federal government, and the framework shows signs of being created to manage complexity.

The ISACA (Information Systems Audit and Control Association) Risk IT Framework and Practitioner Guide [4, 6] is an ISRM/RA approach where the Practitioner Guide complements the Risk IT Framework. The former provides examples of how the concepts from the framework can be realized. It is an established approach developed by ISACA, based on ValIT and CobIT, and, therefore, has a business view on risks, defining several risk areas and factors.

Privacy impact assessments are methods that are supposed to address risks to privacy in a system or a project. The Norwegian Data Protection Authority's (Datatilsynet) *Risk Assessment of Information Systems (RAIS)* [8] are ISRA guidelines that primarily are designed for aiding data handlers in their effort to become compliant with the Norwegian Data Protection and Privacy Act and corresponding regulations.

Outsourcing services to the cloud brings new supplier risks to the organization. Microsoft's *Cloud Risk Decision Framework* [140] is a method for InfoSec risk assessing cloud environments.

12.4 Framework development

The necessity of a bottom-up approach for comparing ISRA methods became apparent when we were studying cause and effect relationships between applying an ISRA method, the work process, and the resulting output. ISRA methods are often comprehensive where comparing tasks and process at a sufficient level of detail is challenging. There exists multiple comparative assessment of ISRM/RA methods [2, 3, 38, 142, 126, 44, 127], however, these are primarily scoped to compare method content to a predetermined set of criteria. These approaches are equivalent of top-down static comparisons and were not sufficiently adaptable. The existing approaches yield differences within the predetermined set of criteria, but will overlook the differences that are not present in the criteria. Which makes them less suited for comprehensively mapping differences between ISRA methods that have items not present in the criteria. In this work, the framework idea is as follows: from our insight into each of the surveyed methods, for each of the methods we identify what issues are covered by the method. Then, we unify of all issues covered by each of the methods. Then, an application of the framework to a risk assessment method amounts first to identify the issues covered by the method and then merging this set with the larger set of issues constructed previously. The assessment of the risk analysis method amounts to investigating to what extent the said method covers all issues present in the super-set constructed previously. The super-set should provide the practitioner with insight into which aspects each method cover, together with an overview of where to seek knowledge in the literature to solve other specific issues or for comparison purposes. Further, we describe the choice of method for framework development, specific CURF development issues, and inclusion/exclusion criteria for the ISRA methods.

12.4.1 Design Science Research

The primary scientific approach applied to develop CURF overlaps with the concepts of the Design Science Research (DSR) methodology. DSR is a problem-solving process specifically designed for research in complex information systems [75]. DSR addresses unsolved research problems experienced by stakeholders within a particular practice and solves them in unique or innovative ways [74] (P. 15). The first step of the DSR process is to define the problem, and, further, to determine the requirements, design, and develop an artifact to address the problem. Followed by a demonstration and an evaluation of the artifact. This study had a defined research problem which needed an artifact to solve it which renders

DSR the obvious choice approach for this study. We both designed the artifact, the comparison framework, and continuously developed and demonstrate it through classification of ISRA methods within the framework and improving the model. We evaluate the model by applying the comparison scheme on the existing methods by adding all standalone tasks, described in Fig. 12.2, and deriving new knowledge. Hevner [74] (P.15) writes that *the key differentiator between professional design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies and the communication of the contribution to the stakeholder communities*. We consider the DSR contribution in this study as primarily the artifact, CURF, which entails a method and the application of CURF to produces a knowledge contribution to the ISRA community.

Recent work on DSR methodology has provided the community with the DSR Knowledge contribution framework [67], which defines DSR contributions within four quadrants. The quadrants are described with *Solution maturity (SoM)* on the Y-axis and *Application Domain Maturity (ADM)* on the X-axis, both scored subjectively using "high" and "low". A high ADM and SoM constitutes a known solution to a known problem, referred to as the routine design. A high SoM and low ADM is an *Exaptation*, where a known solution is applied to a new problem. A low score on both is classified as an invention, as it is a new solution for a new problem. CURF represents a new solution to a known problem, which puts the DSR contribution in the *Improvement* quadrant (low SoM and High ADM). Hence, according to Gregor and Hevner [67], CURF represents both a knowledge contribution and a research opportunity.

12.4.2 CURF Comparisons, Tables, and Scores

The basis for the model was the ISO/IEC 27005:2011 model for ISRM, Fig. 12.1, which holds a level of acceptance in the InfoSec community [157]. The three core activities of the ISRA model consists of *Risk identification*, *Risk Estimation* and *Risk Evaluation*. If a problem was addressed in an ISRA method, but not in the framework, we added it to the model. If a previously added item was partially addressed or mentioned to an extent in a compared method, but not defined as an individual task, we marked it as partially present. In this way, we mapped ISRA processes with coherent tasks and compared the ISRA method to the model to see where they divert and how. This approach allowed for a detailed qualitative comparison of processes and activities in each method and provided a measure of completeness. Each method and concept were evaluated by the authors of this study. We have divided the comparison tables into four tables, whereas Table 12.1 addresses *Risk Identification* related issues. Table 12.2 addresses *Risk Estimation*, and Table 12.3 addresses *Evaluation* related issues. Table 12.4 summarizes the scores and addresses completeness. The two former tables list the identified tasks and activities in the Y-axis and the surveyed methods in the X-axis.

CURF has three scores for each identified task, *Addressed* which is addressed when an issue or task is fully addressed with clear descriptions on how to solve it. *Partially addressed* when an issue or task is mentioned but not substantiated. While the *Not addressed* score is applied for methods that do not mention or address a particular task at all. We converted the scores to numerals for calculations of sum, mean, and averages. The X-axis also has a "Sum"-column which display the total score per row, which is useful to highlight how much emphasis the method authors in sum put on each task and activity.

Also, CURF contains scores on process output from the Risk Identification and Estimation phases; these output criteria are based on best practices and state of the art research on risk assessments [28, 29, 32]. However, we have also added a row of completeness scores without the Output criteria in Table 12.4.

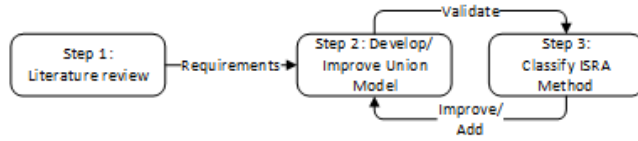


Figure 12.2: CURF development process

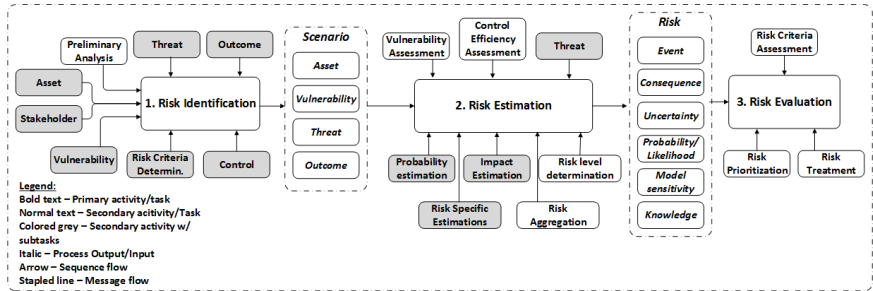


Figure 12.3: Top level of CURF. The generic output of the Risk Evaluation is prioritized risks.

12.4.3 Inclusion and exclusion criteria

The CURF review presented in this paper is by no means a complete overview of existing ISRA methods, as there are over one hundred different ISRA approaches at the current time [127]. We have restricted this study to include eleven methods as it is the idea of CURF which we consider the most important contribution of this research. For the methods included in this study, we chose a set of methods that were easily accessible and which we had prior familiarity. We also added one method developed for cloud [140] on the recommendation from reviewers and one method that focused on privacy risk [8]. The included methods were also not older than fifteen years at a time of review (2016). The studied methods all had their dedicated publication in either peer reviewed channel, standard, or white paper, which contained comprehensive descriptions of work-flow and components. All eleven approaches include risk identification, estimation, and evaluation in some form. In addition, the reviewed methods were either published in English (nine) or Norwegian (two). A path for future work is to expand the framework with additional methods.

12.5 Core Unified Risk Framework (CURF)

In this section, we propose the Core Unified Risk Framework (CURF) for comparing issues in ISRA methods. The issues are grouped into three primary categories; (i) Risk identification, (ii) Estimation, and (iii) Evaluation. Following the method outlined in Section 12.4, we surveyed each of the eleven methods described in Section 12.3 and created the CURF model. Fig. 12.3 is a high-level representation of the results where the colored tasks indicate sub-activities which are described in more detail in the subsequent section. Following, we outline each of CURF's descriptive categories, identified process activities and sub-activities together with the comparison of the eleven ISRA methods for each main process.

12.5.1 Descriptive categories in the framework

To distinguish the ISRA methods, to begin with, we have applied already existing frameworks set them apart. The historical development paths of the multiple risk definitions are an interesting topic which has not been considered in InfoSec. We applied the classification system for risk definitions proposed by Aven [29], which was the only framework available for this type of analysis. He proposes nine classes of risk definitions, out of these nine classes, we found five concepts relevant for our analysis: R as (i) *Expected value* ($R = E$), as (ii) *Probability \times Consequence* ($R = P \times C$), as (iii) *Consequence* ($R = C$), as (iv) *Uncertainty and Consequence* ($R = C \& U$), and lastly, as (v) *the effect of uncertainty on objectives* ($R = ISO$). In addition, we added the Conflicting Incentives Risk Analysis's risk definition, which proposes a risk as conflicting incentives ($R = CI$). The risk definition reveals fundamental properties about the method and the aim of the assessment.

Also, we have added Sandia classifications [44] of each method to indicate the properties of the surveyed functional methods regarding skill level needed. The *Matrix* methods provide look-up tables to support the user, often in the form of software, which requires less expertise from the user. *Assistant* methods provide rich documentation and lists for the user to keep track of the risks but requires a bit more experience. The abstract *Sequential* methods perform tasks in a sequence of activities and require more expertise from the user than the other two. Both the risk definition and the Sandia classification reveal useful properties an ISRA method, hence, they are included in the comparison tables as classifications, but they do not affect the score.

12.5.2 Main process 1: Risk Identification

The main purpose of this process is to identify relevant risk for future assessment. The risk identification process often produces many risk scenarios where some are more likely than others. These identified scenarios are often subject of a vetting process where the main output is the risk scenarios the assessment teams find realistic.

From the development of the unified ISRA model, we found that ISRA methods conduct subsequent tasks at different steps, such as vulnerability assessments may be carried out in either the Risk Identification process and/or the Risk Estimation process. Thus, we only define the vocabulary once, although the definitions are the same throughout the ISRA process according to where the task is conducted. Following is a description of the branches in CURF (Fig. 12.3):

- *Preliminary assessment* (PA) - is the process of conducting a high-level or initial assessment of the ISRA target to obtain an insight into the problems and scope. For example a high-level assessment of assets, vulnerabilities, and threat agents.
- *Risk Criteria determination* (RC) - Deciding on risk criteria for the risk evaluation process, terms of reference by which the significance of risk is assessed. This category includes measurements of risk *tolerance* and *appetite*. Several ISRA also identifies *Business objectives* to aid in scoping the risk assessment and increasing relevance. Risk tolerance and appetite are derived from the objectives. *Key Risk Indicators* build on the predefined appetite, and are metrics showing if the organization is subject to risks that exceed the risk appetite [6]. *Cloud specific risk considerations* are made specifically for cloud migrations and operations, these include issues related to, for example, Infrastructure-, Platform, and Application as a service risks[140].
- *Stakeholder identification* (SI) is the process of identifying and prioritizing the stakeholders that need to be contacted and included in the risk assessment [117, 62, 105]. *Stakeholder Analysis* is the process of analyzing the stakeholders according to relevant criteria, e.g. influence and interest in the project [62].

- *Asset Identification (AI)* is the process of identifying assets, while *asset Evaluation* assess their value and criticality [15]. We have distinguished between *Business process identification* and assets. Identifying the *Asset Owner* helps shape the scope and target of the risk assessment. While *Asset Container* identifies where assets are stored, transported, and processed [46]. *Mapping of Personal data* is a part of the privacy risk assessment process, where the system's handling of information assets containing personal data are mapped and assessed, for example, according to law [8].
- *Vulnerability (Vu) Identification* - The process of identifying vulnerabilities of an asset or a control that can be exploited by one or more threats [12]. *Vulnerability Assessment* is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- *Threat identification (Th)* is the process of identifying relevant threats for the organization. While the *threat Assessment* comprises of methods and approaches to determine the credibility and seriousness of a potential threat [15].
- *Control identification (Co)* is the activity of identifying existing controls in relation to for example asset protection. *Control (efficiency) Assessment* are methods and approaches to determine effectively the existing controls are at mitigating identified risk [15].
- *Outcome identification(Ou)* is the process of identifying the likely outcome of a risk (asset, vulnerability, threat) regarding breaches of confidentiality, integrity, and availability. While *outcome Assessment* incorporates methods and approaches to estimating the potential outcome(s) of an event, often regarding loss [170, 4].

12.5.2.1 Output from Risk Identification Process

Although the risk identification process contains several additional activities, these are not necessarily directly reflected in the risk scenario. For example, existing countermeasures/-controls can be a part of the vulnerability. We define the primary output of the risk identification process is a risk scenario (RS) based on asset (including business processes), vulnerability, threat, and outcome, for which we can compare the methods. We have given scores on these as they are well-developed concepts and important to the granularity of the risk assessment process. For example, an asset can be vulnerable without being threatened, or threatened without being vulnerable. While the *Outcome* is the emphasis on the risk event description, which is important in risk communication [157].

12.5.3 Main process 2: Risk Estimation

The purpose of the risk estimation process is to assign values to the probability and consequence of the risk [15] of the plausible risk scenarios from the identification process. However, reaching realistic estimates of PxC has been one of the major challenges of the InfoSec risk community since the very beginning [164], especially in the quantitative approaches [162]. We have defined the following issues and tasks for the ISRA estimation process (supplemented with issues and tasks from the Risk Identification process):

- *Threat Assessment (TA)*, expands the definition of Risk Identification, the ISRA methods can provide tools to estimate the particular threat agent's (i) *Willingness/ Motivation* to attack [37, 117], (ii) *Capability* in terms of know how[62, 37], (iii) *Capacity* in terms of resources available to conduct the attack[62], and (iv) the potential *Attack duration* which is often related to the consequences of the attack [62, 4, 6]. An example of the latter is the DDoS attack where the outcome of the event will be tightly related to the threats capacity to conduct a long DDoS attack.

Table 12.1: Risk Identification process and output comparison. Scores: XX=2, X=1. Max=22 per row and Max=50 per column

	CIRA [118] 2012 R=CI Sequence	CORAS [105,52] 2006 R=PxC Sequence	GRAMM [170] 2002 R=C Matrix	FAIR [87,62] 2014 R=PxC Sequence	NSMROS [113] 2006 R=PxC Sequence	OCTAVE A [46] 2007 R=C Assistant	ISO/IEC27005 [15] 2011 R=ISO Sequence	NIST 800-30 [37] 2012 R=PxC Sequence	RISK IT [4,6] 2009 R=PxC Assistant	RAIS [8] 2011 R=PxC Sequence	CRDF [140] 2012 R=ISO Sequence	Sum
PA Preliminary Assessment	XX	XX	-	X	XX	XX	-	XX	XX	-	X	14
RC Risk Criteria Determin.	XX	X	X	X	X	XX	XX	-	XX	XX	XX	16
RC Cloud Specific Considera.	-	-	-	XX	-	-	-	X	-	-	XX	5
RC Business Objective Id.	-	X	-	XX	-	XX	-	-	XX	X	X	11
RC Key Risk Indicators	-	-	-	XX	-	-	-	-	XX	-	-	4
SI Stakeholder Identification	XX	XX	-	XX	-	X	-	-	XX	-	XX	13
SI Stakeholder Analysis	XX	-	-	XX	-	-	-	-	X	-	-	5
AI Asset Identification	X	XX	XX	XX	XX	XX	XX	-	XX	XX	-	16
AI Mapping of personal data	X	-	-	X	-	X	X	X	X	XX	-	7
AI Asset Evaluation	X	XX	XX	XX	XX	X	X	X	X	-	-	14
AI Asset Owner & Custod.	XX	X	XX	X	XX	XX	XX	-	-	-	-	10
AI Asset Container	-	X	X	-	-	XX	-	-	-	-	-	4
AI Business Process Id.	-	X	X	-	-	-	-	X	-	-	-	6
Vu Vulnerability Id.	X	XX	XX	X	X	X	XX	XX	X	-	X	14
Vu Vulnerability Assessment	-	XX	XX	-	-	-	XX	XX	X	-	-	10
Th Threat Identification	XX	XX	XX	XX	XX	XX	XX	XX	XX	-	-	18
Th Threat Assessment	XX	XX	XX	-	X	XX	XX	XX	-	-	-	13
Co Control Identification	X	X	-	-	-	X	XX	XX	-	-	XX	9
Co Control Assessment	-	-	-	-	-	-	XX	-	-	-	-	2
Ou Outcome Identification	-	XX	XX	X	XX	XX	XX	XX	XX	XX	XX	19
Ou Outcome Assessment	-	X	XX	-	-	X	XX	-	XX	XX	XX	12
RS Asset,	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	-	18
RS Vulnerability,	X	XX	XX	XX	XX	XX	XX	XX	X	X	X	16
RS Threat,	XX	XX	XX	XX	XX	XX	XX	XX	-	-	-	18
RS Outcome	-	XX	XX	-	XX	XX	XX	XX	XX	XX	XX	18
Completeness	24	33	29	26	21	32	38	24	29	18	18	
XX=Addressed												
x=Partially Addressed												
-=Not Addressed												

- *Probability & Impact Estimation (PI)* - This is one of the main parts of the risk analysis process, where the risk assessors determine the probability and consequence for each identified risk. There are primarily two approaches to probability, frequentist (quantitative) or subjective knowledge-based assessments (qualitative) [29]. The frequentist probability expresses "the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed" [29]. The subjective (qualitative) probability expresses the "assessor's uncertainty (degree of belief) of the occurrence of an event" [29]. Which also relates to *Impact estimation* where the analyst can estimate based on relevant historical data (if it exists), or make knowledge-based estimates of impacts/outcomes. The subjective knowledge-based and frequentist approaches require different activities and are defined as different activities.
- *Risk Specific Estimations (RD)* are method or domain specific estimations. *Privacy Risk estimation* are specific methods to estimate risks to privacy [8]. *Utility & Incentive calculation* addresses issues of utility calculations regarding the risk for each involved stakeholder, and calculate the incentives for acting on a strategy [117]. *Cloud Vendor Assessment* includes methods for assessing the Cloud vendor's existing security controls and compliance [140]. *Opportunity Cost Estimation* are assessments of how much it will cost not to act on an opportunity, by, for example, being too risk averse [117] (P. 99-110).
- The *Risk Aggregation (RAG)* activity is conducted to roll up several linked, often low-level risks into a more general or higher-level risk [37]. During an event, interconnected individual risks can also aggregate into a more severe risk into a worst case scenario. This activity aims to identify and assess such potential developments.
- *Level of risk determination (LRD)* consists of assigning the estimated risk (incident) scenario likelihood and consequences, and compiling a list of risks with assigned value levels [15].

12.5.3.1 Output from the Risk Estimation Process

In terms of risk estimation and evaluation, the key components of a risk (R) related to an activity for discussion and calculation are as follows [28] (p.229) [32]: R is described as a function of events (A), consequences (C), associated uncertainties (U), and probabilities (P). U and P calculations rely on background knowledge (K) which captures the qualitative aspect of the risk, for example, low K about a risk equals more U . Model sensitivities (S) display the underlying dependencies on the variation of the assumptions and conditions. Thus, $R = f(A, C, U, P, S, K)$ allows for a comprehensive output for comparison, as this definition incorporates the most common components of risk and, therefore, constitutes the risk output of the risk evaluation of CURF. For comparison, we have applied the following: C outputs a measure or estimate of consequence. U is an output of uncertainty expressed as a part of the risk measurement, e.g. by calculating the ranges of measurements. The surveyed ISRA method, therefore, needs to apply measurements or frequencies to incorporate U . P relates to both qualitative and quantitative probabilities. S has the same prerequisites as U and is reliant on risk models. The K aspect is present if the method explicitly states that additional knowledge about the risk should be incorporated and applied to adjust the estimations. These have been added to CURF to assist the reader in what to expect as output from using each method.

12.5.4 Main process 3: Risk Evaluation

In this process, the analyzed risks are evaluated and prioritized according to severity. The risk analysis team makes their recommendation regarding treatment of risks, sometimes according to the predefined risk criteria, and the decision-maker decides where to spend the available resources.

Table 12.2: Risk Estimation processes and output comparison. Scores: XX=2, X=1, -=0. Scores Max=22 per row and Max=46 per column

	CIRA	CORAS	CRAMM	FAIR	NSMIROS	OCTAVE A	ISO/IEC27005	NIST 800-30	RISK IT	RAIS	CRDF	Score
AI	-	-	-	-	-	-	-	X	-	-	X	2
TA	XX	-	-	-	-	XX	-	XX	X	XX	-	9
TA	X	-	-	XX	-	-	-	XX	-	XX	-	7
TA	X	-	-	XX	-	X	-	-	-	XX	-	6
TA	-	-	-	XX	-	-	-	-	XX	-	XX	6
Vu	-	-	-	XX	XX	-	-	XX	-	-	-	6
Co	X	-	-	XX	-	-	X	X	-	X	XX	8
PI	-	XX	XX	XX	X	X	XX	XX	XX	XX	XX	18
PI	-	X	-	XX	X	-	XX	XX	XX	X	X	12
PI	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
PI	XX	X	X	XX	XX	X	XX	-	X	XX	-	11
RD	X	-	-	-	-	-	-	X	-	XX	-	4
RD	XX	-	-	-	-	-	-	-	-	-	-	2
RD	-	-	X	-	-	-	-	X	-	-	XX	4
RD	XX	-	-	-	-	-	X	-	XX	-	-	5
LRD	-	-	-	-	-	-	XX	-	XX	-	X	5
Reg	-	-	-	-	-	X	XX	XX	XX	-	-	7
A	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
C	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
U	-	-	-	XX	-	X	X	X	-	-	X	6
P	-	XX	X	XX	XX	X	XX	XX	XX	XX	XX	18
S	-	-	-	XX	-	-	X	-	-	-	-	3
K	X	-	-	XX	-	-	X	X	-	-	-	4
Completeness	17	12	10	30	14	14	23	26	22	20	21	

XX=Addressed
x=Partially Addressed
-=Not Addressed

12. ARTICLE V - A FRAMEWORK FOR ESTIMATING INFORMATION SECURITY RISK ASSESSMENT METHOD COMPLETENESS - CORE UNIFIED RISK FRAMEWORK, CURF

1. *Risk Criteria Assessment (RCA)* - is the process of either creating or revising risk criteria to evaluate risk [117] (P.82).
2. *Risk prioritization/ Evaluation (RPE)* - is the process of evaluating risk significance, and prioritizing for risk treatments and investments [15].
3. *Risk treatment recommendation (RTR)* - is the process of suggesting treatments to assessed risk. This activity is according to ISO/IEC 27000-series conducted as an own process [15], but we have included it here since several of the surveyed ISRA methods suggests treatments as a part of the risk evaluation process [170, 46, 4, 8].

Table 12.3: Risk Evaluation processes and output comparison. Scores: XX=2, X=1, -=0. Scores Max=22 per row and Max=6 per column

		CIRA	CORAS	CRAMM	FAIR	NSMROS	OCTAVE A	ISO/IEC27005	NIST 800-30	RISK IT	RAIS	CRDF	
RCA	Risk Criteria Assessment/Rev.	XX	X	-	-	X	X	X	-	-	-	-	6
RPE	Risk Prioritization Evaluation	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
RTR	Risk Treatment Recommendation	X	-	XX	-	-	XX	-	-	XX	XX	-	9
	Completeness	5	3	4	2	3	5	3	2	4	4	2	
<i>XX=Addressed x=Partially Addr. -=Not Addr.</i>													

12.6 ISRA Method Completeness

The results in tables 12.1 and 12.2 form the basis for the discussion on ISRA method completeness. In this section, we evaluate each surveyed method according to the identified activities based in the CURF, Fig. 12.3.

The process comparison presents a novel approach to comparing ISRA framework based on activities, Table 12.4 displays a measure of ISRA method completeness based on our total results, where we see that the most complete method is ISO/IEC 27005 on the overall. With FAIR scoring highest in the risk estimation process. Following is a summary of differences between the surveyed methods and their completeness.

Table 12.4: Method process completeness according to comparison criteria according to previous scores.

	CIRA	CORAS	CRAMM	FAIR	NSMROS	OCTAVE A	ISO/IEC27005	NIST 800-30	RISK IT	RAIS	CRDF	Max Score
1. Risk Id.	24	33	29	26	21	32	38	24	29	18	18	50
2. Risk Est.	17	12	10	30	14	14	23	26	22	20	21	46
3. Risk Eval.	5	3	4	2	3	5	3	2	4	4	2	6
Completeness Sum	46	48	43	58	38	51	64	52	55	42	41	102
W/O Proc Outcomes	36	34	30	43	24	37	47	38	42	31	31	82

12.6.0.1 CIRA

The Conflicting Incentives Risk Analysis was developed based on Game Theory, Decision Theory, Economics, and Psychology, and is with its utilitarian view entirely different from the other surveyed methods. According to our results, CIRA is a sequential method where the strength lies in the threat actor and stakeholder assessments. CIRA identifies assets, but only for the stakeholders regarding utility, and does not include the more business related activities, although CIRA has been applied to business processes [156]. CIRA does not directly conduct vulnerability and control identification, but threats and stakeholders are at the core of the method.

On R estimation, CIRA is primarily concerned with the threat aspects according to $R = CI$. The method avoids probability calculations and instead estimates utility from executing potential strategies with accompanying outcomes. CIRA also considers opportunity risks. On R evaluation, CIRA addresses risk criteria as defined by the risk tolerance of the risk owner. Also, the method applies an incentive graph for visualizing risk and opportunity.

12.6.0.2 CORAS

CORAS is a sequence method, based on the $R = Px C$ definition; *A risk is the chance of the occurrence of an unwanted incident* [52]. According to our results, CORAS has one of the most complete risk identification processes. The method does not directly address business processes. However, it suggests to map assets into processes and facilitates business process identification as a part of the structured brainstorming process. CORAS does not provide any steps for identifying and assessing existing controls throughout the method, although identifying insufficient controls are a part of the vulnerability identification and the structured brainstorming process. Another strength is that stakeholder communication is emphasized throughout the method.

CORAS lacks most in more advanced threat intelligence activities for risk estimation. Also, CORAS opens for frequentist probabilities [52] (p.56), but is primarily qualitative as probabilities and consequences are estimated in workshop form. For risk evaluation, CORAS makes use of risk matrices.

12.6.0.3 CRAMM

As a matrix method, CRAMM is highly dependent on the accompanying software to provide full support. The $R = C$ definition "Threat * Vulnerability * Asset" does not exclude probability estimations in CRAMMs case. CRAMM is an asset-based method that considers specific threats and vulnerabilities to specific assets. The business and stakeholder-related activities are left out of the method, besides that asset models can be used to reflect business processes. The risk estimation process is primarily based on subjective estimates from experts, but CRAMM also opens for quantifying losses with historical data. CRAMM lacks in all advanced threat intelligence activities for risk estimation. For risk evaluation, CRAMM makes use of risk matrices.

12.6.0.4 FAIR

FAIR is a sequence method, based on the $R = Px C$ definition "*The probable frequency and probable magnitude of future loss*" [62]. Out of the surveyed methods, FAIR stands out as the most dedicated to risk estimation and risk quantification. Which is also the reason for lack of completeness in the risk identification process, such as the business process related activities. FAIR applies a preliminary assessment of assets and threat community to identify risk and produce scenario. The strength of FAIR is in risk estimation, particularly frequentist and quantification, where it is the most mature of the surveyed methods and scores highest in completeness. For example, it considers all aspects of the $R = fA, C, U, P, S, K$ definition, and provides tools for risk measurement and quantification. Threat agent capability is evaluated regarding knowledge and experience requirements, and capacity resources available to the attacker. For risk evaluation, FAIR makes use of several types of risk matrices to articulate risk.

12.6.0.5 NSMROS

The Norwegian Security Authority Risk and Vulnerability Assessment contains is a sequential $Px C$ approach that contains all the fundamental elements of ISRA methods. The NSMROS Risk Identification process is centered on assets, threat, vulnerability, and outcomes, and provides few activities outside of this. The business aspects, such as activities business

processes and stakeholder assessments, are not present in the method. Both the vulnerability assessment and parts of the Risk Estimation process, where the latter is performed as a barrier analysis. The more advanced threat assessment aspects are missing from NSMROS. The method recommends subjective probabilities estimations, but it opens for frequentist approach to probability with a caveat of being aware of forecasting problems. NSMROS suggests gathering loss data to quantify impact estimates. For risk evaluation, NSMROS makes use of risk matrices. The control efficiency assessment (barrier analysis) and stakeholder communication is conducted in the risk treatment phase, after the risk has been estimated and evaluated, and is therefore outside of scope. NSMROS ranks the lowest on our overall completeness measurement.

12.6.0.6 OCTAVE Allegro

OCTAVE Allegro (OA)[46] is the lightweight version of the first OCTAVE, and is an assistant method due to the extensive amount of worksheets it provides to the practitioner. OA bases the risk definition on event, consequence, and uncertainty, $R = C&U$, yet in practice both the method and worksheets put little emphasis on measurements of uncertainty, instead focusing on subjective estimates of consequence in the form of impact areas. Thus, OA is primarily a $R = C$ method. OA is an asset-centric approach, that only considers information as an asset, for example, network infrastructure and hardware are considered as asset containers, which facilitates asset storage and flow. The Risk Identification process in OA scores well on completeness, with the vulnerability, control, and stakeholder assessments as the main areas lacking. OA scores low on completeness in the risk estimation process; with its' primary focus on impact estimation, it does not propose activities to address probability besides a subjective in a worksheet. OA does not address vulnerability and threat assessments in any part of the process. However, the impact estimation is the strong suit of the method. For risk evaluation, OA makes use of risk matrices and also proposes risk treatments as a part of the evaluation.

12.6.0.7 ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management

The ISO/IEC 27005:2011 is a mature ISRM standard which scored the highest on the ISRA completeness measurement. The previous versions of the standard built on a traditional $P \times C$ definition of risk¹, but now applies $R = ISO$ definition as the foundation for the assessment. ISO/IEC 27005 is a sequential method that comes with an extensive appendix, which supports the user in scoping, and asset, threat, and vulnerability assessment. The two only aspects that are not present in the risk identification process are key risk indicators, asset containers, preliminary assessment, and stakeholder analysis. The vulnerability and threat assessments are described as part of the identification processes and supplemented in the Annex, and we, therefore, consider these as full activities in the risk identification process. In the Risk Estimation process, the standard does not address the specific threat assessment activities as a part of the process. ISO/IEC 27005 does contain a description of how to conduct both a subjective knowledge-based and frequentist probabilities and impact estimations. However, for the latter, it does require prior knowledge of statistics. For R , the standard mentions uncertainty, model sensitivity, and knowledge aspects as the degree of confidence in estimates. In the Risk Evaluation process, the predefined risk criteria are applied to the analyzed risks and proposes several types of matrices for risk evaluation and prioritization.

¹"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 regarding a combination of the probability of occurrence of an event and its consequence", - ISO:IEC 27005:2008

12.6.0.8 NIST Special Publication 800-30, Revision X- Guide for Conducting Risk Assessments

The NIST SP 800-30 R.1 [37] is a sequential method based on the $R = PxC$ definition of risk. The 800-30 scored in the bottom range of the Risk Identification process completeness. It is a threat-centric method, which creates a notable absence in asset identification and evaluation processes. Assets are mentioned in conjunction with other tasks, especially threat identification, but not considered as either a main or secondary activity. The method suggests a threat-based approach to risk, instead of an asset-based approach. SP 800-30 also lacks tasks for outcome and stakeholder assessments. In the Risk Estimation process, the method partially identifies assets and has a comprehensive threat assessment process. It supports both subjective knowledge-based and frequentist probability estimations or a combination of the two. NIST SP 800-30 only supports subjective impact estimations regarding affected assets from the risk. The method allows for different risk models, and the components of the estimation output are dependent on the chosen model. All this results in the method scoring the second highest on completeness for the Risk Estimation process. In the Risk Evaluation process, NIST SP 800-30 suggests to evaluate and prioritize risk in tables consisting of several descriptive categories.

12.6.0.9 The Risk IT Framework and Practitioner Guide

ISACA's Risk IT qualifies as an assistant method due to the extensive documentation it provides, based on the $R = PxC$ definition of risk. Risk IT scores the second highest in completeness, but it is the least accessible of the surveyed literature, it took us quite some time to get an overview of the content and process. An example of the method being hard to access is that assets are required to produce the risk scenarios, but there is no particular activity to identify or evaluate the assets. It is a business centered method that covers all business-related aspects of the ISRA process, also bringing *risk indicators* into CURF. Risk IT provides a lot of tools and descriptions for the user which makes it score well on the completeness measurement. For the Risk Identification process, Risk IT centers on the development of risk scenarios, consisting of actors, threat type, event, asset/resource, and time. One problem is that the authors partly mix up the terminology, for example, the suggestions for events include both adverse outcomes and vulnerabilities, which are not the same thing. The scenario focus is also possibly the reason for the ISRA activities being hard to identify, whereas several tasks are embedded into others (the most comprehensive description of the process is in [4] p. 65-76). Risk IT does not include activities for control and threat assessment in the risk identification process. In the Risk Estimation process, Risk IT does not consider the threat assessment activities, but it contributes to the model with considerations of *attack duration*. Risk IT advice both frequentist and qualitative assessments, or a combination of the two, both probability and impact. In the Risk Evaluation, Risk IT proposes to rank risks with risk matrices, but also to evaluate through peer reviewing inside the company as a quality assurance process.

12.6.0.10 Privacy Risk Assessment of Information Systems (RAIS)

RAIS is a sequential PxC that has been scoped primarily for assessing privacy risks; it is an asset-centric approach where the emphasis is on identification and security of personal information. The method comes with domain-specific tools for mapping and evaluating personal data, and provides guidelines for qualitative descriptions of privacy impact. Therefore, adds two additional categories to CURF; (i) Mapping of personal data and (ii) Privacy Risk Estimation. The risk identification process in RAIS scores the lowest of any method, primarily due to the lack of focus on vulnerability, threat, and controls. However, the RAIS threat assessment tools provided for the risk estimation process are comprehensive, together with a well-described process for estimating PxC , which makes the method score high in completeness for risk estimation. The main drawbacks of the method are that

it overall lacks tools for control and vulnerability analysis. RAIS emphasizes risk criteria and acceptable risk as one of the starting points for the assessment but does not suggest to revise these in the risk evaluation phase.

12.6.0.11 Microsoft Cloud Risk Decision Framework (MCRDF)

MCRDF [140] is a sequential method built on the ISO/IEC 31000-standard for generic risk management and applies the $R = ISO$ definition of risk. MCRDF is an ISRA for the cloud is scoped to support in the decision-making regarding cloud-based risks. The method adds two cloud-based categories to CURF; (i) Cloud specific risk domains (risk identification) and (ii) Cloud Vendor Assessment (risk analysis).

Our analysis of the content shows that it scores low on completeness regarding common InfoSec-related tasks, such as asset evaluations and threat assessment. The strong side of MCRDF is the overview of cloud-associated risks control areas and the detailed example for applying the method. The method provides easy-to-apply examples of qualitative PxC calculation examples, which are grounded in the risk control areas. One drawback with MCRDF is that it is too dependent of the tables, and does not provide additional approaches for identifying and managing risks that are outside of the risk control areas.

12.7 Scope and Limitations of the current ISRA methods

One of our most significant findings is that no method is complete in CURF. The method we consider most complete is ISO/IEC 27005:2011 which addresses several issues in some way, but for example, falls short when compared to FAIR's detailed risk assessment approach. The following discussion will first analyze the scope of ISRA methods, then row scores, and, lastly, the presence of modern risk concepts in the surveyed ISRA methods. In tables 12.1, 12.2, and 12.3, we also summed each row to show where the area of focus for ISRA developers lie. We apply the priority ranges 0-7 = low, 8-15 = medium, and 16-22 = high, to simplify discussion.

12.7.1 ISRA Method development scope

Analyzing the row scores reveals which areas the ISRA method developers prioritize. ISRA have previously had a tendency to have a too technical scope and not address the needs of the organization [164]. Although this may be improving as an overall [157], we see from organizational and business-related categories, RC and SI, that these issues have not been a high priority in the development of methods. Besides, only ISO/IEC 27005 fully identifies business processes as assets to the organization.

The only issue addressed by all methods in the Risk Identification process is threat identification. Followed by the outcome, asset and vulnerability identification, which provides an indicator of what the output of the process should contain. Control identification and assessment are conducted in both the Risk Identification and Estimation parts of the ISRA, the sum of which equals existing controls in the high priority range. NSMROS suggests to do the control assessment as a part of the *Risk Treatment* process, which we consider as too late, as the existing controls have a direct influence on the risk level.

Based on the high degree of threat focus in the risk identification phase, the diverse approaches to the different threat assessment categories is surprising. NIST 800-30 markets itself as a threat-based risk assessment method but seems not to prioritize asset evaluation. The results also show a difference in *PxI* approach; where the qualitative methods are more utilized, especially for impact estimations. Related to threat motivation lies game theoretic-based estimations of utility and Incentives for risk estimates, which is a field largely ignored in the surveyed ISRA methods besides CIRA.

On the risk estimation itself, our results show that all methods consider event(s) and consequences. Most methods include some form of probability while very few address un-

certainty beyond probability. Descriptions of risk model sensitivity have a model-based method as a prerequisite and is primarily an issue of quantitative methods, and is only considered FAIR. While four methods partially address the knowledge aspect, leaving *S* and *K*-aspects in the low priority range.

The Risk Criteria determination requires the risk criteria to be defined in risk identification process and is, therefore, limited to those methods. All methods conduct risk prioritization and evaluation. While only a few propose risk treatments as a part of the risk evaluation process, common to run this as an own process, see Fig. 12.1).

Based on this analysis, the development scope of ISRA methods centers on asset, vulnerability, threat, and controls. The development also tends to be turning towards more business related aspects. The main direction of risk assessments, besides FAIR, are developing aspects of qualitative risk assessments and methodologies for generic and specific estimations. Further, we will analyze the row scores and go deeper into each specific area.

12.7.2 CURF Row Scores

In CURF's *Risk Identification* part, Table 12.1, asset, threat, vulnerability, and control identification and assessments all score highly in CURF, while threat scores are highest. However, an analysis of the identified parts of the threat assessment in the *Risk Estimation* table (12.2, show that there is no unity on what is important to consider in these assessments. CURF summed up the issues concerning threat willingness/motivation, capability, capacity, and attack durations, but no methods addressed all of these aspects on its own or propose an approach to operationalizing them.

Further, Risk Criteria is partially or fully dealt with in all but one of the surveyed methods. These are criteria for risk evaluation and decision-making late in the process. Only four methods address the criteria in the *Risk Evaluation*, Table 12.3. One issue with defining the risk criteria this early and not revising later, is that when it comes to the decision-making, it is entirely up to the decision-maker(s) to consider if it is acceptable. In our experience, the risk criteria function as heuristics for the risk assessors but are not static. The severity of the risk is not the only factor that determines whether or not it is acceptable. For example, the cost of mitigating the threat may be too high, and, therefore, sways the decision to acceptance of a risk that was deemed unacceptable by the risk criteria. Thus, the cost/benefit analysis of the risk treatment is also an important factor to consider besides the criteria. Besides risk criteria, the RC tasks of CURF score in the medium to low range. For example, *Key risk indicators* are also only addressed by two methods, which are strongly tied to key performance indicators in business. Further strengthening the RC area of methods will assist in practitioner business understanding by mapping risk indicators and understanding business processes, and assist the integration of the ISRA program into the organization.

Five of the methods either propose business processes as an asset or as a central part of the risk assessment, but does not discuss the issue that protecting business processes is far more complex than protecting an asset. Although, as discussed understanding business processes are important in recognizing organizational context. Mapping out and modeling business processes require a lot of resources and will create a substantial overhead on the ISRA process at the lower abstraction layers.

CURF also shows that *Stakeholder identification* is increasingly being implemented into ISRA methods. Gathering data on who knows what and how to contact them is important, especially for the assessments not reliant on penetration tests for data collection.

Cloud specific considerations is only fully considered by the CRDF and FAIR, one of which is genre-specific for cloud. Both of the two genre specific-methods, cloud [140] and privacy [8], shows that they rely on the ISRM fundamentals, but add tasks to CURF that are unique to them. Examples are *Privacy risk estimation* and *Cloud vendor assessment*. FAIR is one the only generic ISRA method we found to consider cloud issues specifically. The ISO-standards do address these issues, but not the surveyed ISO27005 for ISRA.

The RS row scores in the risk identification phase show asset, threat, and the outcome being

included equally, while vulnerability scores two points lower. However, two risk methods [62, 113], suggest conducting the vulnerability assessment primarily in the risk estimation process, which suggests that these four areas are treated equally.

From CURF's Risk Estimation table, we see that there is a diverse amount of tasks and few areas in which most of the methods overlap. The two most significantly overlapping areas are subjective probability and impact estimation, the latter is one of two tasks that has a full score in CURF. Quantitative estimates of P and C have the second highest scores, while the remainder of tasks is spread among the different methods. CURF shows that the most addressed area in risk estimation are $P \times C$ calculations, while the remaining RD categories are largely specific to the method that introduced it. Among the other types of estimations, the Utility and Incentive calculations in CIRA are closely related to threat motivation but goes deeper into these aspects by applying economic theory to threat estimation. Besides CIRA, understanding human nature is an important point that seems largely neglected by the ISRA methods. Only two approaches address the cost of lost opportunities as well. From the Risk Evaluation table, CURF shows that *Risk Prioritization/Evaluation* is the top priority of this process. From the reviewed methods, consideration of incentives is limited to CIRA.

To summarize, the business related RC and SI areas in CURF currently presents limitations to several methods. Threat assessments have the highest priority in CURF, but there are diverse approaches to what should be risk assessed, and no method covered all aspects within the TA category. The four RD categories consistently scored low and were specific to the methods that introduced them.

12.7.3 Existing methods and modern risk concepts

Several modern concepts from generic risk literature are yet to make an impact in the ISRM methodologies. Besides FAIR's Montecarlo-based approach and ALE/SLE models (Annual and Single Loss Expectancy), there is little information on the ISRA methods on how to obtain quantitative probabilities. Related to risk quantification is the Black Swan concept proposed by Taleb [144]. None of the ISRA methods addresses Black Swan risks although the complexity and interconnectivity of the ICT systems keep growing, making them more susceptible to Black Swan events. Actively estimating risk aggregation and cascades are one mitigating activity that may reduce the impact of Black Swans. Wangen and Shalaginov [162] and Hole and Netland [79] have proposed more specific approaches for incorporating this issue into ISRA and, but these have yet to be adopted into methods.

Knowledge about risk, K , is also mostly left out of the ISRA methods, meaning the descriptions of the background knowledge and assumptions that U and P are based on. As an example, a risk assessment shows a small probability of a particular threat agent committing a distributed denial-of-service (DDoS) attack occurring the coming year. Consequently, the risk will also be low. However, if the probability is based on weak knowledge and assumptions, the risk should perhaps be considered as higher. Descriptions of K are particularly important for risk estimations regarding complex systems where knowledge is limited. None of the reviewed methods addresses this aspect in full.

12.8 Relationship to other literature

In this section, we discuss the previous work conducted by others in the research field and how the method and results in this paper differ and extends previously published work. There are several comparison studies of ISRM/RA methods in the related work. We have previously referenced the Sandia Report [44] which presents a classification scheme where ISRM methods are sorted in a 3-by-3 matrix by the level of expertise required and type of approach. The Sandia classification adds complements our results by stipulating the level of skill needed to apply an ISRA method. The historical and recent development trends of

the risk concept proposed by Aven [29] also complements this framework by providing the background and foundation of each risk approach.

There exist multiple comparative studies outlining ISRA approach content to aid organizations in choosing a method, for example, ENISA's high-level summary of existing methods [2] and *Methodology for evaluating usage and comparison of risk assessment and risk management items* [3]. The latter is a well-developed approach for comparing and benchmarking possible ISRM processes, together with expected inputs and outputs. The benchmark follows the classic ISRM process (Fig. 12.1), including the six main ISRM stages and fifteen defined sub-process. There are several resemblances to CURF in the comparison method, for example, both have the ISO/IEC 27005 as a starting point and apply a similar scoring system. However, they are also different as the ENISA method compares to a set of items that we interpret as best practices, while CURF compares with items present in methods, and grows if the new item is added. The former ENISA comparison [2] is a high-level comparison of methods, based on four predefined categories for ISRM and ISRA, eight in total. While similarly, Syalim et.al [142] has published a comparative analysis that applies four predefined generic steps of the ISRA process for comparison. Both these studies compare a set of ISRA methods within a predefined set of criteria. An approach that risks leaving important aspects out of the comparison. For example, both comparisons downplay the role of the asset identification and evaluation process, which, often is the foundation of the risk assessment. The results in our paper differ from these in that ours are versatile and adaptable; allowing for other tasks and activities beyond predefined categories to be added and analyzed. In this context, Bornman and Labuschagne [38] presents a very detailed framework for comparing the complete ISRM process, divided into five categories, where the *Processes* category is interesting for our work. The authors built their comparison criteria on CobiT (*Control Objectives for Information and Related Technology* (COBIT) by ISACA). This framework focuses on what the compared methods address and contains about COBIT, but not differences in how they recommend solving the task, or the distinct differences between the approaches.

Another similar study was conducted by Shamala et.al. [126] which defines a detailed information structure for ISRA methodology contents. This comparative framework was developed to evaluate ISRA methods primarily on the information structure regarding what is needed at a particular step in the assessment. The contents of the framework are derived from a detailed comparison of popular ISRM/RA methods, and, therefore, has a similar approach to our work, but with a different purpose and scope, and, therefore, different results regarding criteria. Whereas Shamala et.al. focuses on how and what information to collect, our results look at how ISRA methods address particular tasks and issues.

Agrawal [17] has published a comparative study of ISRA methods, in which the author summarizes four methods using ontology. The paper compares the four ISRA methods to eight pre-defined criteria, whereas it considers if a method is primarily qualitative or quantitative, purpose, and if it is scalable. Agrawal also describes the expected input, effort, and outcome of each process step, and then discusses the pros and cons of each reviewed method. This study overlaps with CURF in some of the criteria, such as methodology, outcome, and the use of Sandia Classification [44]. However, the main methodology and approach to the problem are different, as Agrawal also considers a set of predefined criteria for each method.

One of the most comprehensive taxonomies of ISRA regarding reviewed methods is the Shamel-Sendi et.al. [127] study, in which the authors have reviewed 125 papers. The study provides a modern taxonomy of ISRA methods based on a set of four categories identified by the authors. The first category, *Appraisalment*, is defined as the type of input and output of the risk calculation, such as if it is qualitative, quantitative, or a combination of both (hybrid). The second category addresses the ISRA method's *Perspective*, which is either business, asset, or service-driven. An additional category, *Threat-driven* [37], could also have been considered for the perspective category. The third category, *Resource val-*

uation, which primarily considers how the ISRA method suggests evaluating valuables: either asset, service, or business process, and if it considers functional dependencies between them. Whereas compromising one asset may inflict consequences on another, and such on. The fourth category is *Risk Measurement* in which the taxonomy classifies ISRA methods regarding how they consider impact propagation, meaning if the method advises considering an impact only to the asset itself (non-propagated) or if it considers dependency between assets and other resources. The Shameli-Sendi et.al. taxonomy considers how an ISRA method classifies within the predefined criteria identified by the authors, while CURF compares on criteria and tasks present in the methods. Both approaches aim to assist practitioners and organizations in the choice of ISRA approach, while Shameli-Sendi et.al. is at a higher level of abstraction addressing four core issues in ISRA, CURF provides in-depth analysis of how well each method addresses each task. Thus, these two approaches have complementary features.

On the topic of research problems, both Wangen and Snekenes [164] and Fenz et.al. [58] 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 related work contains several approaches to comparing method content. However, these are primarily studies of properties and content based on a predefined set of criteria. None of which address how to compare full ISRA processes and content beyond these criteria. Thus, the gap in the research literature lies in the lack of a bottom-up approach to compare ISRM/RA methods. The main difference between these results and our findings is the method applied to categorize; all of the previous work has classified work within predefined categories, which is a top-down approach. While our classifications have been developed and evolved inductively through surveying methods, only predefining the three primary risk processes, and growing each subset according to the surveyed literature.

12.9 Conclusions

To conclude this paper, we have presented CURF, which was developed inductively through reviewing eleven well documented ISRA methods; CIRA, CORAS, CRAMM, FAIR, NSM ROS, OCTAVE, ISO/IEC 27005:2011, NIST SP 800-30, and Risk IT, in addition to two domain-specific methods, one for cloud, CRDF, and one for privacy, RAIS. Literature studies show that there exist multiple comparative assessments of ISRM/RA methods, but these are all scoped to compare method contents to a predefined set of criteria, equivalent to a top-down approach. For most cases, this is less flexible concerning addressing issues missing in the predefined criteria. With CURF we have shown the utility of comparing methods and building the framework from a bottom-up point of view. Our results, therefore, consists of a larger superset of issues and tasks from all reviewed ISRA methods using ISO/IEC 27005:2011 as a reference point, and then comparing the ISRA methods as a measure of completeness covering all the issues and activities added to the superset. The possibility to add new problems makes our proposed framework highly flexible to changes in future methods and comparing methods that are very different.

No evaluated method is complete in CURF, but from all of the methods reviewed, ISO/IEC 27005:2011 is the most complete and covers most issues in one way or another. However, FAIR was the most complete method risk estimation. Another finding is that beside FAIR, there is little information on how to obtain quantitative probabilities in any of the ISRA methods reviewed. There are several ISRA frameworks and practices, however, we find variations of asset evaluation, threat, vulnerability and control assessments at the core of the most reviewed frameworks. While the more specific issues, such as cloud risk assessment, is primarily addressed by methods developed for that purpose. It was also interesting to find that none of the ISRA methods discuss the presence of unknown unknowns

(Black Swans), which is highly relevant due to the dynamic and rapid changes in ICT systems, which only are growing and getting more complex. Beside CIRA, the human motivational element of InfoSec and ICT systems seems mostly neglected.

12.9.1 Limitations & Future Work

CURF has limitations in the abstraction layer as we chose to keep the comparison at a high-level, the model does not display deeper differences between methods such as specific approaches to asset identification, vulnerability assessments, and risk estimation. For example, the new version of FAIR [62] comes with a detailed approach to risk estimation, while other methods that appear somewhat equal in the comparison, such as NSMROS [113], only describes the activity with at a high abstraction. Which means that a closer study of the methods and a possible expansion of the tables will reveal deeper differences in scope and methodology not present in our work. This includes the time-parameter for *PxI* calculations suggested by one of the reviewers. A possible addition to the framework is to expand it with experience-based knowledge and to grow it by making it available to other scholars and practitioners. Comprehensiveness of activities and accessibility of the ISRA methods is not considered in this comparison, which are issues we uncovered for some of the frameworks. Another limitation is that, although, for example, ISO 27005:2011 scored low on the cloud specific criteria, third party management is covered in the supporting material (ISO/IEC 27001 and 27002 standards). This may also be true for other reviewed methods.

Further, this work highlights the need for a more thorough discussion on what the different aspects of an ISRA should consist of, such as threat and control assessments.

Acknowledgments

The Ph.D. student Gaute Wangen acknowledges the sponsorship from the COINS Research School for Information Security. The authors also acknowledge the excellent feedback and contributions from the anonymous reviewers.

Article VI - Information Security Risk Assessment: A Method Comparison

Gaute Wangen

*Information Security Risk Assessment: A Method Comparison. IEEE Computer Magazine Special Issue: Cyber Physical Systems and Security Risk Assessment, 2017, 50(4), 52-61.*¹

13.1 Abstract

Information security risk assessments (ISRA) are performed daily according to different standards and industry methodologies, but how does the choice of a method affect the assessment process and its end results? This research qualitatively investigates the observable differences in effects from choosing one method over another. Through multiple empirical case studies, our work compares the application of three ISRA methods. We first outline the theoretical differences between the three methods and then analyze the experience data collected from the risk assessment teams. Finally, we examine the metadata of the produced risk assessments to identify differences. Our study found that the choice of a method influences the assessment process, along with its outcome.

Keywords:Information Security, Risk Assessment, Case study.

13.2 Introduction

Currently, there are numerous information security (InfoSec) risk assessment (ISRA) methods to choose from [127], but scarce information on how to choose and if this choice matter for the result. Since multiple ISRA approaches exist, it is in the interest of the InfoSec community if this choice matters for the outcome, both for improving decision basis, increasing security levels and maximizing return on investment. This paper compares three different ISRA methods; *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro* (OA) [46] and *ISO/IEC 27005:2011 - Information Security Risk Management* (ISO27005) [15], together with one Norwegian method; *Norwegian National Security Authority (NSM) Guidelines in Risk and Vulnerability Assessments (NSMROS)* [113]. This study considers three types of empirical comparisons; comparison through practice, method content, and the produced results from application. The data for this study was collected through multiple risk assessment case studies in a Norwegian academic institution. Firstly, we apply the results from Core Unified Risk Framework (CURF) [161] to define distinctiveness of each method. Secondly, we collect and analyze experience data from ISRA groups. Finally, we apply CURF in a novel way to compare ISRA metadata results. While numerous studies of ISRA methods exist [127, 126, 164], this is the first study that we are aware of in which the methods are practically applied and compared. The main benefit of this paper is new knowledge regarding ISRA method performance, both in the results and experiences with the methods, in addition to our proposed comparison method establishing cause-effect relationships. The scope of this study is limited to risk assessment and treatment as defined

¹The forthcoming version in IEEE Computer Magazine has been edited to fit the style and requirements of the publication channel.

in the ISO 27000-standards [11, 15].

The following section describes the necessary background information and terminology used in this paper for the reader to be able to follow. The related work primarily contains a presentation of CURF and differences between the three ISRA methods. Furthermore, we present the research method, which describes the case studies, empirical data collection, and analysis of both experience data and ISRA results. Finally, we present the results and analysis of the experience data and the ISRA reports using CURF, before discussing the results and concluding the paper.

13.3 Background and Related Work

This section presents a summary of the fundamental concepts for understanding the ISRA discipline and the terminology applied to the remainder of this article. In addition, we introduce the previous work that has motivated this study, in particular, CURF and the included ISRA methods.

13.3.1 Information security risk assessments

InfoSec risk comes from applying technology to information [36] and 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 [11]. Best practice InfoSec is highly dependent on well-functioning ISRM processes [36] which is the practice of continuously identifying, reviewing, treating and monitoring risks to achieve risk acceptance [15]. Risks for information systems are defined as an adverse event with estimations of consequence (C) for the organization (e.g. financial loss) and the corresponding probability (P) of the event occurring. Further, the ISRA results are assessed by the decision-maker, and if found unacceptable, steps are taken to mitigate the risk to the organization. A *risk assessment* consists of the overall process of risk analysis and risk evaluation [11], and *risk analysis* is the *systematic use of information to identify sources to estimate the risk*[11]. Risk evaluation is the *process of comparing the estimated risk against given risk criteria to determine the significance of the risk* [11], while risk treatment represents the chosen strategy to address an unacceptable risk.

13.3.2 CURF and included ISRA Methods

Several frameworks exist for theoretically comparing ISRM/RA methods with each other (e.g. [127, 126]). However, the existing approaches are primarily scoped to evaluate ISRA content to a predetermined set of criteria, which is equivalent to a top-down approach and quite restrictive as differences not present in the criteria will be overlooked. This scheme makes them less suited for analyzing cause-effect relationships between method and results, since causes not present in the criteria may be neglected. The CURF bottom-up approach [161] solves this problem by mapping ISRA method content and using it as comparison criteria. For each added method reviewed in CURF, we identify which tasks the approach covers and combine all the tasks covered by all surveyed methods into a combined set. The evaluation of the ISRA method consists of investigating to what extent the said method covers all undertakings present in the already created super-set. This approach makes CURF a bottom-up comprehensive comparison where the criteria are determined by the method tasks rather than being pre-determined. The included ISRA approaches are functional and formal ISRA methods that focus on assessments of assets, threats, and protections, often with measures of P and C [44]. CURF has three scores for each identified task: *Addressed* when a task is fully addressed with clear descriptions on how to solve it, *Partially addressed* when an undertaking is mentioned but not substantiated, and *Not addressed* for methods that do not mention or address a particular task at all. CURF provides a measure of completeness for the studied methods, see bottom row in Table 13.1.

Table 13.1 highlights how the approaches differ, where the summary of each column shows completeness. The row scores reveal how well the ISRA methods scored overall. The three ISRA methods included in this study was also used as input for developing CURF (see [161]), following is a summary of each method and their differences.

Table 13.1: CURF, main qualitative differences between frameworks

	NSMROS	OCTAVE A	ISO/IEC27005	Row Sum
<i>Risk Identification</i>				
Preliminary Assessment	2	2	0	4
Risk Criteria Determination	1	2	2	5
Business Objective Identification	0	2	2	4
Stakeholder Identification	0	1	2	3
Asset Identification	2	2	2	6
Mapping of personal data	0	1	1	2
Asset Evaluation	2	1	1	4
Asset Owner & Custodian	0	2	2	4
Asset Container	0	2	0	2
Business Process Identification	0	0	2	2
Vulnerability Identification	1	1	2	4
Vulnerability Assessment	0	0	2	2
Threat Identification	2	2	2	6
Threat Assessment	1	2	2	5
Control Identification	0	1	2	3
Control Assessment	0	0	2	2
Outcome Identification	2	2	2	6
<i>RI Completeness</i>	13	23	38	
<i>Risk Estimation</i>				
Threat Willingness/Motivation	0	2	2	4
Threat Capability (know how)	0	0	1	1
Threat Capacity (Resources)	0	1	1	2
Vulnerability Assessment	2	0	0	2
Qualitative Probability Est.	1	1	2	4
Quantitative Probability Est.	1	0	2	3
Quantitative Impact Estimation	2	1	2	5
Qualitative Impact Estimation	2	2	2	6
Level of risk determination	0	0	2	2
Risk Aggregation	0	1	2	3
<i>RA Completeness</i>	8	8	16	
<i>Risk Evaluation</i>				
Risk Prioritization/Evaluation	2	2	2	6
Risk Treatment Recommendation	0	2	0	2
<i>RE Comp</i>	2	4	2	
<i>Completeness</i>	23	35	46	
2=Addressed 1=Partially Addressed 0=Not Addressed				

13.3.2.1 NSMROS

The Norwegian NSMROS [113] was derived from the Norwegian Security Act for compliance purposes. We initially applied NSMROS because our teams were Norwegian and the method had a good standing in the Norwegian ISRA community. NSMROS is a sequential [44] probabilistic approach centered on assets protection, threat, and vulnerability, and provides few activities outside of this.

13.3.2.2 OCTAVE Allegro (OA)

is a lightweight version of the original OCTAVE and was designed as a streamlined process to facilitate risk assessments, and reduce the need for InfoSec experts while still producing robust results [46]. OA was recommended to us by several experts in the field as an established method with several academic citations and references. OA is a checklist approach (*assistant*[44]) due to the amount of worksheets it provides to the practitioner. In OA a risk is an event with corresponding consequence and uncertainty. Instead of probability, OA instead focuses on subjective estimates of consequence in the form of impact areas.

13.3.2.3 ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management [15]

details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood. The ISO27005 scored the highest on the ISRA completeness measurement [161], Table 13.1. We chose to include the ISO/IEC 27005:2011 as it is regarded as the best practice standard for ISRM. ISO27005 is a sequential method that comes with an extensive appendix, supporting the user in scoping the assessment, and the asset, threat, and vulnerability assessments.

13.4 Method

This study includes the results from four case studies conducted with each method and twelve risk assessments in total collected over five years. For the case studies, we had independent risk assessment teams running projects primarily at the strategic and tactical level at an educational institution. Each group conducted one assessment using one primary method for their project. Further, we collected and compared the experience data from the groups using interviews and questionnaires. Lastly, we applied CURF to analyze the resulting risk assessment report and to establish a cause-effect relationship between method and result. The following subsections substantiate each step in the research process.

13.4.1 Research design

The case studies were risk assessments of real-world targets in an academic institution as a part of a mandatory ISRM course. The local IT organization provided the assignments and made available resources to assist the projects. The end reports were the primary deliverable and used in the local ISRM program for decision-making. Each case study was performed by a homogeneous group of InfoSec students, with group sizes ranging from six to ten participants. All of the participants had received basic training in InfoSec, but had no experience following formal ISRA methodologies. All groups completed a six-week basic ISRA training before conducting the primary task. The researchers participated as supervisors and subject-matter experts. All the groups followed one method, completed their risk assessment projects within four months, and presented their findings to the decision-makers. The groups primarily used interviews and online sources for data collection, supplemented with questionnaires, observations, and sampling. The experiment did not allow technical tools for active penetration testing. Each group delivered their findings in a final report, which outlined identified risks, analysis, and proposed treatments. The groups applied one ISRA method but were given access to supplementing literature which they could use as needed.

13.4.2 Data collection and Sample

We designed a survey to collect qualitative experience data at the end of each project. Key areas of interest were experiences with applying each method, how the groups used it, together with advantages/disadvantages of the method. The survey also mapped each groups dependency on supporting literature. As for the level of measurement, the instrument had category, ordinal, open-ended, and continuous type questions. Category for demographics and categorical analysis, while the main bulk of questions were designed using open-ended and ranking questions, with the latter using the Likert scale *1 - Not at all, 2 - Low, 3 - Medium, 4 - High, and 5 - Very high*. For NSMROS and ISO27005, we ran the data collection as an online questionnaire, while we conducted face to face interviews with the OA groups. In total, this study incorporates 26 answers to questionnaires, and four group interviews including 8-10 people per interview.

13.4.3 Qualitative Data Analysis

For *Descriptive analysis* we have considered distributions using the median together with range, minimum-maximum values, and variance. We also conducted *Univariate* analysis of individual issues, and *Bivariate* analysis for pairs of questions to see how they compare and interact. This study also analyses the distributions of the answers, for example, if they are normal, uniform, bimodal, or similar. *Crosstabulation* was applied to analyze the association between two category type questions. The survey had several open-ended questions which we have treated by listing and categorizing the responses. Further, we counted the occurrence of each theme and summarized the responses.

13.4.4 Risk Assessment Report Analysis

Since the variety of targets for the risk assessments was too diverse to compare findings, instead we studied the focus areas and metadata. For each of the four ISRA reports produced with each method, we applied the CURF bottom up approach and mapped the contents of each report and combined them for comparison with the other methods. Each identified area, e.g. "Threat Assessment," was scored by the same system as CURF (not addressed - 0, partially - 1, and addressed - 2). Since we had four reports for each method, we qualitatively assessed each report and added the total score (maximum 8) for each method for comparison. In order to make the theoretical and risk reports results comparable, we assigned the following ranges: 0-2 equals *Not Addressed*, 3-5 equals *Partially addressed*, and 6-8 equals *Addressed*.

13.5 Experiences using the ISRA methods

This section summarizes the experiences reported by groups using NSMROS, OA, and ISO27005, presented in that order. We start with the reported advantages and disadvantages of applying each method, before discussing the method's appendices, customization, use of supporting literature, and data collection.

13.5.1 Advantages and disadvantages of each method

Our results show that the participants were equally satisfied with their methods, all perceived as 4 - *Highly Useful*, where NSMROS received the single lowest score (2 - *Low*) and ISO27005 the highest (5 - *Very high*). Our results showed that the reported difference in perceived usefulness between the ISRA methods was minimal. Table 13.2 summarizes the advantages and disadvantages from using each method.

13.5.1.1 NSMROS

was easy to understand and apply, where the two most frequently mentioned points was that the process was well explained and defined, together with being sequential and easy to follow. Besides, the method was reported to be versatile with easy-to-distribute tasks. NSMROS was also reported to be easy to use and well suited for beginners. Another advantage was that NSMROS is written in the native language which made it easier to understand.

The main disadvantages was that the how-to description of each step in the method was scarce with insufficient explanations of key tasks. There was also a lack of examples both in the text and from other sources which made the process hard to follow.

13.5.1.2 OA

had several advantages, such as being easy to follow with a systematic and comprehensive process. Regarding the latter point, the OA checklist approach created a rigorous assess-

13. ARTICLE VI - INFORMATION SECURITY RISK ASSESSMENT: A METHOD COMPARISON

ment, which also forced the groups to research areas that else could have been overlooked. The focus on organizational drivers was a positive trait of the method as it forced a better organizational understanding. The groups also reported consequence estimation as one of OA's strong suits. The groups also said that OA is easy to apply once they had learned it. The overall assessment was that the worksheets and templates worked well to support their risk assessments.

On the reported disadvantages, all groups reported OA to be hard to understand and learn because it was overwhelming and the non-native technical language left more room for misunderstanding. All groups found the organizational drivers hard to define, and the time spent working on the drivers may not have been worth the effort. OA was also too rigid and dependent on the worksheets, which caused some of the groups to get stuck on tasks just producing worksheets. One example of this is that OA requires one schema per critical asset. OA is a rigid methodology and requires one task to be completed before starting the next, which hindered efficiency in the large groups and limited the opportunity for conducting parallel tasks. The groups reported that the lack of focus on probabilities made it hard to differentiate, prioritize, and communicate risk with equal consequence. All groups also reported the project to have too many participants (8-10) to apply OA.

13.5.1.3 ISO27005

main advantage was a comprehensive task, process descriptions, detailed approaches, and ISO27005 on an overall was perceived as a useful tool for ISRA. Regarding the process descriptions, the groups found the clearly described inputs and outputs of each process particularly useful. ISO27005 was reported as well structured, easy to look up and use as a point of reference. The groups also easily found existing examples of applications and checklist templates on what to include in the analysis useful. The standard was easy to apply in practice and provided a nice introduction to ISRA.

The main disadvantages with ISO27005 were that it was a challenging read and hard to grasp for novices caused by the extensive use of technical expressions, interpretations, and technical terminology. The comprehensiveness of the framework made it hard to find relevant information, learn, and understand. These issues were especially prominent when the groups were working on understanding the tasks, finding where to begin, and scoping the project. The eight groups working with ISO27005 and OA all struggled with the technical non-native language of the methods.

13.5.2 Method Independence

All three included methods adhered to the practice of describing the primary process in the main document and then substantiate each step in the appendices. This part first analyzes the usefulness of the appendices of each method, before investigating how the groups applied supplementing literature for their assessments.

13.5.2.1 Appendices and Supplementary material

The appendices in NSMROS are primarily worksheets addressing ISRA planning, asset and system identification, and risk identification. The NSMROS groups reported a low usefulness overall for the appendices. The OA Worksheets (Appendix B) and Example Worksheets (Appendix D) covers assets, risk criteria, impact areas, and risk estimation, and were both reported as highly useful. The groups considered supplementary method guidance (Appendix A) as medium useful in the ISRA project. None of the groups made use of the questionnaire worksheet (C).

ISO27005 has five primary appendices: Annex A is intended to assist the practitioner in scoping the assessment. (B) addresses asset identification and evaluation, (C) addresses threat identification, (D) addresses vulnerability identification and assessment, and (E) pro-

vides strategies and tools for performing an ISRA. All the ISO27005 Appendices were perceived as useful. Although the median was three (medium) for all the appendices, the results show that eight or more of the respondents found Annex B and C high or very highly useful.

13.5.2.2 Use of Supplementing literature

One of the premises of the study was that the groups had access to a set of supplementing literature in a shared repository together with open sources. We asked the participants about their reliance on supporting literature for the risk assessment. All groups frequently applied the local security policy and principles document in their assessment. However, supporting literature was not frequently used overall. For the NSMROS groups, ISO27001 was most often used together with ISO27002. The OA groups primarily used supplementing literature for *PxC* calculations and to derive organizational drivers. The ISO27005 groups reported that they sometimes used the foreign and domestic threat assessments together with native language resources. As an overall, the need for supporting literature seemed consistent and similar with all three approaches. The noticeable difference is that ISO27001 was used more frequently with the NSMROS groups. Another difference is that the OA and ISO27005 groups scored higher on native language ISRA resources. The right column in Table 13.2 summarizes the reported needs covered with supplementing literature for each approach.

Table 13.2: Summary of reported advantages, disadvantages, and needs covered with supporting literature from each method

	Advantage	Disadvantage	Supplementing Literature
<i>NSMROS</i>	<ul style="list-style-type: none"> - Well defined sequential process - Well explained process - Nice introduction to ISRA - Easy to distribute tasks - Native language 	<ul style="list-style-type: none"> - Too generic task descriptions - Lack of examples - Vague estimation metrics 	<ul style="list-style-type: none"> - Templates - Examples - How-to ISRA - Scoping
<i>OCT A</i>	<ul style="list-style-type: none"> - Adaptable - Systematic and comprehensive process - Worksheets - Easy to use once learned 	<ul style="list-style-type: none"> - Hard to learn and understand - Probability not prioritized - Too rigid 	<ul style="list-style-type: none"> - Probability - Asset evaluation - Threat identification - Organizational Drivers - ISRA explanations in native language
<i>ISO27k5</i>	<ul style="list-style-type: none"> - Detailed descriptions - Well structured - Nice reference - Easy to apply 	<ul style="list-style-type: none"> - Heavy reading - Hard to grasp - A lot of irrelevant info for one ISRA project 	<ul style="list-style-type: none"> - Threat assessments - <i>PxC</i> Estimations - Terminology - Definitions - ISRA explanations in native language

13.6 Analysis and Discussion

This section first presents the comparison of CURF and the ISRA reports. Secondly, we compare the experienced differences with CURF.

13.6.1 Differences in the Risk Assessment Reports

Having outlined the differences in ISRA method application, this study proceeds to analyze differences in ISRA reports. We applied the CURF approach to assessing the qualitative differences in the risk assessment results and identified twenty-six documented tasks in the reports. Table 13.3 outlines the tasks and the overall qualitative differences in the content of the delivered reports; the completeness score reveals a clear difference between the methods with the ISO27005 groups scoring the highest.

13. ARTICLE VI - INFORMATION SECURITY RISK ASSESSMENT: A METHOD COMPARISON

Table 13.3: Observable differences in the risk assessment reports. Max score 8 per method, 24 per row, and with 26 identified tasks, and 208 per column.

Tasks	Subtasks from Report	Source	NSMROS	OA	ISO	Row
Case Description	Organizational Drivers	OA	6	2	4	12
	Risk Measurement Criteria	C	7	8	8	23
	Organizational Goals/ Business objectives	C	4	5	8	17
Risk Identification	Stakeholder Identification	C	8	8	8	16
	Asset identification	C	6	8	8	22
	Asset evaluation/Criticality	C	3	8	8	19
	Asset Container	C	0	7	3	10
	Threat Identification	C	4	8	8	20
	Threat Assessment	C	1	3	8	12
	Areas of concern/ Vulnerability identification	C	8	8	8	24
	Vulnerability assessment	C	5	0	8	13
	Control identification	C	4	0	8	12
	Control assessment	C	0	0	6	6
	Outcome identification	C	8	8	8	24
Risk Estimation	Impact Area Prioritization	OA	4	8	3	15
	Threat motivation	C	0	6	7	13
	Threat Capability	C	0	0	7	7
	Threat Capacity	C	0	0	7	7
	Qualitative Consequence Estimation	C	8	8	8	24
	Qualitative Probability Estimation	C	7	7	8	22
	Risk Scenarios	C	8	8	8	24
Risk Matrix/table	C	7	6	7	20	
Risk treatment	Risk Prioritization	C	7	8	8	23
	Treatment plan	C	8	8	8	24
	Cost/benefit analysis	OA,JSO	6	8	8	22
	Residual Risk	ISO	4	4	6	14
Completeness Score			121	148	184	

Table 13.4 compares each ISRA method’s theoretical CURF scores to the observed results in the delivered risk reports. The content of the table was constructed from the observable contents of the reports and supplied with tasks from CURF, in total seventy-eight comparisons. The analysis assumes that a successful prediction includes both addressed and partially addressed tasks for both CURF and the reports, or a double absent. An unsuccessful prediction then constitutes occurrences where a task was present in one but not the other. Basing the analysis on this assumption, CURF predicted sixty-five out of the seventy-eight tasks documented in the reports, including nine double absent. In total, there were twelve unsuccessful predictions regarding tasks present in the reports but not in CURF. Further, we found that some of the technical tasks from Table 13.1 were not included in the reports: Any conducted *Preliminary assessment* was not documented in the reports, nor had any of the groups recorded work with *Business process identification*, *Risk Quantification*, or *Risk aggregation*. The three latter tasks are alternative and advanced approaches which limited their usefulness for the novices in the study and were not necessary for completing the project. Besides these four tasks, no fully *addressed* tasks in CURF were ignored in the reports. The results in Table 13.3 shows that having a task adequately addressed in the ISRA method influences the content of the report and vice versa. Some notable examples: we see from the analysis of NSMROS that leaving the threat and control assessment out of the method resulted in them being left out of the report. OA does not include a vulnerability assessment scheme which produced four reports without it. However, there are some exceptions; an unmentioned task in CURF was adequately addressed in the reports in two instances: NSMROS *Stakeholder identification* and OA *Cost/benefit analysis*; These tasks were necessary to complete the risk assessment, for example, all the groups were dependent on interviews for data collection and needed to know the stakeholders to run their projects. Another example was organizational understanding using NSMROS, which does not pro-

vide any detail on how to achieve this objective. However, we saw from the reports that all the NSMROS groups had worked with risk criteria and to some degree with understanding organizational business objectives. Another issue with NSMROS was that proposing to conduct the control efficiency assessment after the risk evaluation is completed resulted in none of the NSMROS groups doing it. Thus, the sequence of ISRA tasks also matters for the results.

Table 13.4: Comparison of observable theoretical differences from CURF and differences in reports. *XX=Addressed, X=Partially addressed, & 0=Not addressed*

Task	NSMROS		OCTAVE A		ISO27005	
	CURF	Report	CURF	Report	CURF	Report
Case descr.						
Organizational Dr. Risk Measurement Criteria	0	X	XX	XX	0	X
Org. Goals/ Business objectives	X	XX	XX	XX	XX	XX
Risk Identi.						
Stakeholder Id.	0	XX	X	XX	XX	XX
Asset Identification	XX	XX	XX	XX	XX	XX
Asset Evaluation	XX	X	X	XX	X	XX
Asset Container	0	0	XX	XX	0	X
Threat Identification	XX	X	XX	XX	XX	XX
Threat Assessment	X	0	XX	X	XX	XX
Areas of concern/ Vulnerability Id.	X	XX	X	XX	XX	XX
Vulnerability assessm.	0	X	0	0	XX	XX
Control identification	0	X	X	0	XX	XX
Control assessment	0	0	0	0	XX	XX
Outcome identification	XX	XX	XX	XX	XX	XX
Risk Est.						
Impact Area Pri.	0	X	XX	XX	0	X
Threat motivation	0	0	XX	XX	XX	XX
Threat Capability	0	0	0	0	X	XX
Threat Capacity	0	0	0	0	X	XX
Qualitative Conseq. Estimation	XX	XX	XX	XX	XX	XX
Qualitative Prob. Estimation	X	XX	X	XX	XX	XX
Risk Scenarios	XX	XX	XX	XX	XX	XX
Risk Matrix/table	XX	XX	XX	XX	XX	XX
Risk Eval. & Treatment						
Risk Prioritization	XX	XX	XX	XX	XX	XX
Treatment plan	XX	XX	XX	XX	XX	XX
Cost/benefit analysis	XX	XX	0	XX	X	XX
Residual Risk	X	X	XX	X	XX	XX
<i>Total Results (CURF-Rep.)</i>	<i>Occurrences (Total 78)</i>					
	XX-XX	40	XX-X	5	X-XX	11
	X-X	1	X-0	2	0-0	9
	0-X	8	0-XX	2		

13.6.2 Experienced differences

The critique we gathered of each method had few overlaps with the technical differences: We found that all the risk assessment groups preferred templates and examples: the OA groups ranked the worksheets as most helpful, and the other groups actively looked for templates and examples in other sources. However, one of the drawbacks of the OA worksheets was the amount of paperwork and extra overhead they created.

Both the ISO27005 and OA groups sought out mother tongue sources to compensate for the technical non-native language, indicating that technical language was a hindrance for usability. Another practical difference was that the NSMROS groups primarily looked for templates and examples on how to conduct ISRA, together with information on how to scope the assessment.

OA also introduces the identification of organizational drivers as a task. However, all groups struggled with defining the drivers and separating them from organizational vision, mission, goals and key performance indicators. Although understanding the organization is highlighted in both OA and ISO27005, our results indicate that the guidelines are

not sufficiently substantiated for novices.

ISO27005 came out best in CURF and was clearly stronger in practice when it comes to threat, vulnerability, and control assessments. All the delivered ISO27005 reports were consistently better at describing these areas, and the groups were satisfied with the descriptions of these areas. However, some of the other issues encountered by all the groups were already known in the academic literature [164, 159], such as difficulties with PxC estimations, organizational alignment, and asset evaluation. Our results show that these tasks are still difficult even when described well in the methodology. In particular, the lack of probability calculations in OA created practical problems for all the groups, due to not being able to prioritize risks with the same consequence and distinct difference in the rate of occurrence.

To summarize, user-friendliness was primarily what the groups cared about, including templates, understandable language, and how-to descriptions. There were observable differences between the work processes of applying each method, and several of these differences are also documented in Table 13.3.

Our study also found common issues to all ISRA methods, especially related to data collection, information gathering, and analysis. Such as knowing what data to collect, analysis of interviews, and response rates on questionnaires. Furthermore, all groups struggled with general stakeholder management, such as scheduling interviews, knowing who to interview, various communication issues, and discovering credible sources beyond the interviews.

13.7 Conclusion

Our results show that the choice of ISRA method does matter both regarding content, experience, and produced results. Our novel application of CURF to analyze metadata worked well to establish a cause-effect relationship between ISRA tasks and results. Besides, we found a clear relationship between method and report completeness, whereas the ISO27005 groups scored highest. When inexperienced risk assessors apply a method, its content matters strongly for both the ISRA process and outcome. A lot of the feedback on the use of methods was related to user-friendliness and not related to process or tasks. However, some issues are universal and should be prepared for, such as data collection issues with analysis and stakeholder management. Besides, the necessity of some tasks for succeeding forced the practitioners to conduct them whether they were present in the framework or not. The participating groups also favored easy to learn methods with checklists and examples, which are desirable items to include into ISRA methods. Our results should strengthen the research incentive within specific ISRA areas, in particular, method development and usability, tools for organizational understanding, and ISRA application and comparison.

13.7.1 Limitations & Future Work

One limitation of this study was that we had different case studies for each group, which limited our ability to isolate the method variable regarding ISRA results. Another limitation of our data is that they were gathered from novices and may not apply for specialists and experts. However, we know from experience that on-site personnel and non-specialists often conduct ISRA, for whom, the method is essential, and our results do apply. Using students has its limitations; first, they have diverse interest and ability, which determines the quality of the result. Secondly, most of the groups needed guidance to complete the assignment, which may lead to supervisors influencing the results. The sample size is an issue in resource intensive qualitative studies; although the results were strongly indicative, four reports per method may not be enough evidence to conclude. Another limitation was that we had a delay for experience data collection with the NSMROS groups, which caused

fewer participants to share their experiences.

Data collection is crucial for the ISRA, and a path for future research is studies of data collection methods and techniques for making the ISRA more efficient. Since CURF still is an innovative approach and not fully developed, further development and expansion of CURF is also possible. We showed in the report assessments that the model is adaptable. However, the idea of CURF can be applied for other comparisons and expanded further by adding more nodes in the tree, for example, expanding with the issues uncovered through practical experience. Lastly, we encourage others to conduct similar studies and these will benefit the ISRA community by determining what works and what does not.

Acknowledgments

The author thanks Christoffer V. Hallstensen, Nils Kalstad Svendsen, Stian Husemoen, Ole Ingarth Langfeldt, NTNU IT, Einar Snekkenes, the anonymous reviewers, Sarah Louise Bergdølmo, Dimitra Anastasopoulou, and the A-IMT1132 students from 2010-2016.

Article VII - Quantitative Risk, Statistical methods, and the Four Quadrants for Information Security

Gaute Wangen & Andrii Shalaginov

Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers, Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security, Springer International Publishing, 2016, 127-143.

14.1 Abstract

Achieving the quantitative risk assessment has long been an elusive problem in information security, where the subjective and qualitative assessments dominate. This paper discusses the appropriateness of statistical and quantitative methods for information security risk management. Through case studies, we discuss different types of risks in terms of quantitative risk assessment, grappling with how to obtain distributions of both probability and consequence for the risks. N.N. Taleb's concepts of the Black Swan and the Four Quadrants provides the foundation for our approach and classification. We apply these concepts to determine where it is appropriate to apply quantitative methods, and where we should exert caution in our predictions. Our primary contribution is a treatise on different types of risk calculations, and a classification of information security threats within the Four Quadrants.

Keywords: Risk Assessment, Information Security, Statistical Methods, Probability, Four Quadrants, Black Swan

14.2 Introduction

Being able to predict events and outcomes provide a great benefit for decision-making in both life and business environments. For information security risk management (ISRM), the aim is to find the appropriate balance in risk-taking relative to the organization's risk appetite and tolerance. Too many security controls will inhibit business functionality, and the opposite will lead to unacceptable exposure. The inherent complexity of information communication technology (ICT) makes it challenging to gather enough relevant data on information risks for building statistical models and making quantitative risks calculations [26]. It is therefore generally perceived as being too much work, complex and time-consuming [164]. However, we argue that the cause for the lack of prevalence of statistical methods is just as much lack of maturity in the field as the reasons stated above. Prediction of information security risks has therefore been reliant on the intuition and heuristics of the subject matter experts [26, 164]. Although qualitative methods are the predominant approach to forecasting information risks, there is ample evidence from psychological experiments suggesting that qualitative risk predictions are unreliable [144, 89, 164]. Moreover, the qualitative risk analysis is not suitable when dealing with expected monetary

losses such that Annualized Loss Expectancy. Quantitative and statistical methods should provide better results than guesswork and improve decisions in the long run. However, there are many types of information risks, and it is not likely that we can predict all equally well. Information security risks are more often than not products of complex systems and active adversaries. The main topics in Black Swan [144] is risk unpredictability caused by lack of data and knowledge about the complexity and the limitations of statistical methods in predicting risks in such systems. Lack of understanding and overconfidence in models often leads to the costly mistake of underestimating risk. The Four Quadrants [143] is a risk classification system developed primarily for economics for determining where the risk analyst safely can apply statistical methods, where he should show caution, and where to discard traditional statistical approaches. In this article, Taleb's Four Quadrants are adapted to address the feasibility of applying statistical methods to predict information risks. To the extent of our knowledge, there has not been published any previous work on this particular issue.

To provide a clear view on the problem, we did a feasibility study of applying statistical methods to several major information risk case studies that can affect any businesses or even countries. This work addresses the following research questions and finds answers with relevant support from the case studies: (i) *Can we apply statistical methods to deal with Information Security Risks? Sketch the applicability domains and possible failures to predict extreme events* and (ii) *In which information security domains can statistical methods be applied to improve the decision-making process in risk management even if the methods do not seem reliable and accurate?* The implication from answering these research questions are both theoretical, corresponding knowledge and historical data was collected, simulated and analyzed in this study. For practical implications, a family of various statistical approaches was analyzed with scientifically sound proof for specific methods and applications for ISRM even if the prediction results are not entirely reliable. Furthermore, we discuss factors that contribute to our lack of knowledge about the quantitative ISRM using statistical methods as the most promising approach to numerical characterization of the ICT risks. Additionally, a classification of risks within the Four Quadrants is proposed.

The remainder of this article is as follows: First; we present the state of the art in ISRM in the Section 14.3, define the terminology and describe the Four Quadrants classification scheme. In the Section 14.4 we describe the applied method. We present three case studies and their relation to quantitative risk assessment and their relation to the Four Quadrants in Section 14.5. Section 14.6 discusses our findings, factors that reduce predictability, and classification of information risks within the Four Quadrants. The conclusion is found in Section 14.7.

14.3 Information Security and Risk Assessment

ISO/IEC 27005:2008 defines information or ICT risk in as *the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization*. Probabilistic risk analysis (PRA) is the preferred approach to risk in information security. Where impact to the organization (e.g. loss if a risk occurred) and probability calculations of occurrence express risk. There are no standardized statistical approaches to information risks. To calculate risks (R) we, therefore, apply the definitions provided by Aven in [28] (p.229) for discussion and risk calculation. Where risk is described by events (A), consequences (C), associated uncertainties (U) and probabilities (P). U and P calculations rely on background knowledge (K). Also, model sensitivities (S) are included to show how dependencies on the variation of the assumptions and conditions. Thus, $R=f(A, C, U, P, S, K)$. A quantitative risk assessment in this sense derives from applying statistical tools and formal methods, mainly based on historical data (e.g. law of large numbers), obtained distributions and simulations. So, based on the definition of risk by Aven, we will consider applications of relevant methods for quantitative risk evaluation in terms of R. A risk as-

assessment is very seldom purely quantitative as there are assumptions K underlying the forecast. Exposure is a crucial concept in risk management that we define as how susceptible an organization is to a particular risk.

14.3.1 The Black Swan and the Four Quadrants

N.N. Taleb [144] developed Black Swan theory to describe rare, extreme and unpredictable events of enormous consequence. These events, known as Black Swans, are so rare that they are impossible to predict, and they go beyond the realm of reasonable expectations. A Black Swan has three properties; (i) It is an outlier. (ii) It carries an extreme impact. (iii) Moreover, despite its outlier status, human nature makes us formulate explanations for its occurrence after the fact, rendering it explainable and predictable. The Four Quadrants risk classification concept comes from the core concepts of the Black Swan, which links risk management to decision theory. *The classification system allows us to isolate situations in which forecasting needs to be suspended or a revision of the decision or exposure may be necessary* [143], and to determine where it is safe to apply statistical risk models. The classification consists of two types of randomness and decisions [143, 144]:

Mediocristan randomness is predictable; the Gaussian bell curve applies and applying statistical methods is safe. Examples of *Mediocristan* are human height, weight and age probability distributions, where no single outcome can dramatically change the mean. We can accurately predict events in *Mediocristan* with a little uncertainty, e.g. hardware lifetimes are from *Mediocristan*. *Mediocristan* randomness represents risks in Quadrants 1 and 3 in the classification.

In *Extremistan* randomness is Black Swan domain where small probabilities and rare extreme events rule. Since samples of events are so rare, the probability models will be sensitive to minor calculations changes and prone to error. In *Extremistan*, events scale and are subject to *fat-tails*¹, and can appear as power law or Pareto distributions. An example of such an event is the development of the amount of malware in the wild, with a growth trend that follows a Pareto distribution, where the theoretical malware amount is close to infinity. *Extremistan* randomness represents risks in Quadrants 2 and 4 of the classification.

The two types of payoffs from decision making are; (1) Simple Payoffs and (2) Complex Payoffs. In the former, decisions are binary form, e.g. either true or false, infected or not infected, which is where mainly probabilities play. Decisions are more complex for the latter, where the decision-maker must also consider the impact or a function of the impact, and weight benefits against disadvantages. Type 1 is thin-tailed and non-scalable while type 2 decisions can be fat-tailed.

This accumulates into Taleb's risk classification system of four quadrants; where risks in the First Quadrant has *Mediocristan* randomness and low exposure to extreme events. The payoffs are simple and statistical models work. Exposure to events in the Second Quadrant comes with *Mediocristan* randomness with complex payoffs, where it is generally safe to apply statistical models, factoring in awareness of possible incomplete models. Exposure to Third Quadrant risks comes with *Extremistan* randomness and low exposure to extreme events. The Fourth Quadrant is *"the area in which both the magnitude of forecast errors is large, and the sensitivity to those errors is consequential"* [143].

14.3.1.1 The Black Swan and Four Quadrants in ICT Risk

For explicitly information security risk, the Black Swan concept has been treated by Hole and Netland [79], who treats the subject of risk assessing large-impact and rare events in ICT. Where the authors provide a basic discussion of what black and gray swans are in information systems and discuss events that may qualify as Swans. They define cascading risks and single points of failure as sources for swans, viruses, and other malware are

¹In comparison to the Normal distribution a Fat-tailed distribution exhibits large skewness or kurtosis.

sources for cascading risks. Additionally, Hole [78] addresses how to manage hidden risks, and how to recover quickly from Black Swan ICT incidents. Audestad (P.28-37) [26] discusses the limitations of statistics from an information security perspective. Audestad does not apply the term Black Swans, but he briefly discusses extreme events and limitations of statistics.

14.4 Methodology for statistical risk analysis and classification of events

The primary approach for the feasibility study in this paper is theoretical and statistical analysis of several types of information risks by considering a set of related cases that accompanied by historical data. The main classification scheme that we follow in the case study is the Four Quadrants as described by Taleb [143, 144]. The work to classify risks within the Four Quadrants consisted of gathering data and analyzing information security risks to determine their properties, and if statistical data is available if it would be appropriate to run calculations. The motivation is to use conventional statistical methods with a hope to extract particular characteristics that are suitable for quantitative risk analysis and further Threat Intelligence and Threat Forecasts. Additionally, we make a hypothesis about the applicability of a particular method. The information risks we have addressed were chosen from ISO/IEC 27005:2011, and we consider risks towards entities and not persons. This work focuses on risks from the compromise of information, technical failures, and unauthorized actions and does not address risks posed by natural events or similar. The calculations in this article are based on acquired data published by others. Furthermore, we perform specific statistical tests of whether such models are applicable for historical data or not, and extract corresponding quantitative measures. Our approach focuses on usefulness and limitations of statistical methods for information security risks analysis and predictability. In particular, we have analyzed risks to determine their properties with respect to the Four Quadrants (randomness and payoff). The following subsection describes the statistical methods and probabilistic models applied in this paper.

14.4.1 Supplementary statistical methods for historical data analytic

One makes a decision about information security risks mostly based on the previously collected data within the company or based on the publically available historical data about causes and results [91]. We introduce several community-accepted methods to deal with historical data and be able of making quantitative risk assessment possible since qualitative risk assessment has precision limitations when it is necessary to make predictions in numbers.

Probabilistic modeling. This type of analysis is applied when it is a need for probability estimation of a particular event x occurrence in a given historical dataset. Initially, the model $p(x)$ is built, and an estimation of the corresponding set of parameters from the data [65]. Then, this model can be used to estimate the probability of similar events in this very period or later on. We can state that there exist many obstacles related to the probabilistic modeling. First, very few data points from history may cause a wrong decision. Second, very rare events, like in the case of Fourth Quadrant, have negligibly small probabilities. However, this does not mean that this event are not going to happen.

Numerical analysis. Numerical analysis is a broad field of data modeling, in particular, time series. The function $f(x)$ is build using previous period of time x_0, \dots, x_t . To construct a proper model, available historical data have to be decomposed into trends, seasonal components, and noise in order to build a precise prediction model. At this point, the recent data should possess the biggest degree of trust rather than data from a long time before [24]. For the defined earlier research questions that statistical models can be applied

to support risk assessment within the four quadrants, yet under some limitations, we consider the following supplementary statistical approaches [24] from the previous Section:

1. **Logistics function** describes the process when the initial impact causes exponential increase until some moment of time. After this moment, the growth will be decreasing until it is saturated to some ceiling value [54].
2. **Conditional Probability** and **Bayes Theorem** are the probability methods used to calculate the likelihood of occurrence of some event when another dependent or independent event already happen.
3. **Gamma distribution** represents a family of continuous probability distributions that can describe data with quite various characteristics. The main parameters are shaped k and scale of the distribution θ .
4. **Exponential growth** characterize an event that does not have an upper boundary, and the observed outcome will grow more during the next period in comparison to previous.
5. **Log-normal probabilistic model** defines the distribution of some historical data under the condition that the logarithm of the data follows the Gaussian distribution.

So, these methods are the most promising from our point of view for estimation of possible event outcomes based on the previously analyzed information.

Statistical hypothesis testing. Further for each case study we will justify the usage of specific statistical methods and make a hypothesis about their applicability in that particular case. At this point, we need to use statistical tests to verify suggested hypothesis². The two following approaches can be applied with probability distributions: QQ-PLOT, a Quantile-Quantile plot represents a probability plot by depicting expected theoretical quantiles E and observed practical quantiles O against each other and STATISTICAL TESTS that estimates the quantitative metrics of how well the data fit hypothesized distributions.

Confidence Intervals or CI relates to the probabilistic estimation of whether a particular data or data sample is being placed within a hypothesized distribution. It also means that the defined in CI % of data will be in the hypothesized distribution. To be precise, the tests evaluates the actual observed data O with the expected data E from the hypothesized distribution.

14.5 Case Studies

In this Section, we answer RQ 1 and show the application of models for ISRA with corresponding failures and Confidence Intervals (CI). This study is a comprehensive overview since a particular Case may require several methods to give a broader model. Our approach discusses specific types of risk for information security and where risks can be computed using statistical methods. We characterize information risks by the following predicate:

$$\textit{Malicious Intentions} \xrightarrow{\textit{Action}} \textit{Observable Outcomes} \quad (14.1)$$

Since the original *Malicious Intentions* may not be known, the quantitative risk analysis relies on the historical data about *Observable Outcomes* that can be either published by the information security labs or available within an organization. Each risk calculation in the following case studies are made for the purpose of illustrating and discussing the risks properties, and all risks are considered from the viewpoint of an organization. Based on the publicly available sources of information we made tentative calculations to give our answers on the research questions. Although not present in this paper, we have also explicitly treated risks of Insider attacks and phishing for the classification.

²<http://www.ats.ucla.edu/stat/stata/whatstat/whatstat.htm>

14.5.1 Advanced Persistent Threats (APT) and Cyber Industrial Espionage

APT are professional, resourceful and global actors often supported by Nation-States. These threats conduct targeted attacks over extended periods, aiming to compromise institutions for through cyber espionage and sabotage.

There are several problems when risk assessing APT attacks; tailored malware and techniques, making signature based scanners obsolete, and detection extremely resource intensive. APTs are generally very low probability (few incidents), although some companies daily deal with this threat. Modus operandi for APTs is stealth and extract data unnoticed, and even with a large ongoing compromise, the target's operations will be business as usual, making losses hard to visualize. Observing the severity of an APT breach is only possible after an extended period, which makes consequences both hard to predict and communicate. There are several different potential outcomes ranging from benign to malicious, all associated with a considerable amount of uncertainty. The discovery of an incident will have consequences, the "Initial Shock", where the harm comes from the loss of resources from general incident handling to before returning to normal. From there, the future of the incident has a large amount of variables affecting the outcome, all with their associated uncertainties. For example if the stolen data was production information, we must consider the probability of product replication, and what harm this would bring to the company in the future. Meaning that without extensive knowledge about the attacker and historical data, we cannot assign probabilities to these variables. Thus, there is a significant amount of uncertainty related to APT attacks.

We propose the following answer to the RQ1 for APTs:

- *Data source.* Targeted organizations generally do not reveal much information about APT. Therefore, the statistics for the particular events and actions are not shown to the public, and most data are available in vague numbers after the damage done. Therefore, the only data we can rely on to deduce the exact flow of the attack can be the analysis reports published by the security labs.
- *Discussion of statistical approach.* Since the exact data in most cases are unavailable or not computable, we can rely on the potential outcomes of the APT attacks. At this point as independent variable *Time* comes after the initial shock. The dependent variable, *Consequence*, therefore follow the numerical analysis model (1) LOGISTIC FUNCTION since at the beginning the range of probable outcomes growth exponentially until it reaches some point, where the attack approaches maximum damage. Ideally, it will grow as an (2) EXPONENTIAL FUNCTION, yet in real life there are logical boundaries unless cascading happens.

In Fig. 14.1 we have modeled an APT incident; after the initial shock, the system returns to normal, and the uncertainty of the damage is growing until the consequences become evident. Therefore, we conclude that the best way to describe this process is to use Logistic Function, where dependent on the type of business the harm (Y-axis) must reach a maximum amount after some time.

- *Results - Uncertainty/ Confidence intervals.* The second problem when estimating the risks of APT is the Confidence Interval (CI) estimation of the risk management decision. The uncertainty of the attacks against organization increases after the evidence of the initial attack, which makes the confidence interval of the predicted risk value too low to rely on it:

$$R|_{CI} \approx \frac{1}{uncertainty} \quad (14.2)$$

Bigger uncertainty causes less confidence in the predicted outcomes of the damage done. The larger range, the harder to estimate final risk and make an appropriate risk management decisions.

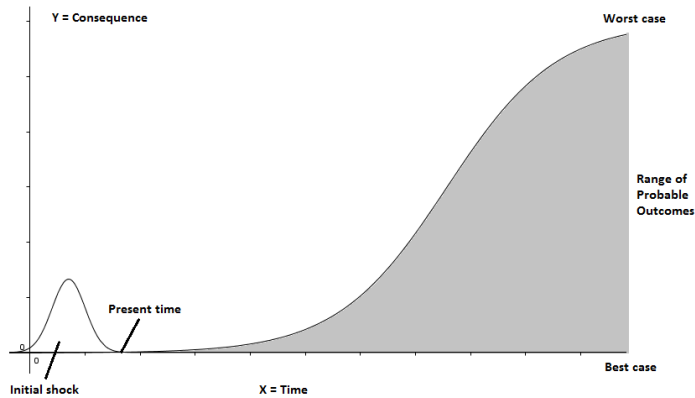


Figure 14.1: Example of potential outcomes from an APT/Espionage attack, $Y = \text{Consequence}$ $X = \text{Time}$. The initial shock comes from detecting and responding to the breach. The long-term C is represented as a Logistic function, where P of all A are bound with a close to unsolvable U.

- *Results - Applicability of statistical methods and possible failures for each risk.* Since no data available, it is hard to derive any meaningful decision from the unreliable model that follows EXPONENTIAL FUNCTION. At this point, we do not have any other sources to rely on, so this model helps to understand the way of damage developing. Also, we may derive the qualitative prediction using monotonicity of the process development. This model can be used (1) to show the importance of finding the attack evidences and cause in the initial phase, and (2) impossibility to say the exact cause in the final stage until it is obvious.
- *Classification of Risk -* Without knowledge about attacker intentions and capabilities, a victim of an APT attack, particularly industrial espionage, can only make risk predictions based on knowledge about internal processes and the value of the stolen information. Even if the Logistic function corresponds to the nature of the APT harm, it is still rather a random prediction than reliable results for risk analysis. No outcomes of an APT attack will be identical, and outcomes are complex in nature, prone to cumulative effects. There is also a lack of both data and knowledge about attacks with corresponding consequences, which makes it a *Fourth Quadrant* risk.

14.5.2 Malware and Botnet distributions

Successful malware distributions such as different versions of botnets, e.g. Zeus, Conficker³ and others, have shown considerable resilience towards eradication. Epidemic models have proven useful for estimating propagation rates [171, 26], however, historical data is more useful for obtaining probability distributions. We propose the following answer to the RQ1 for Malware and Botnet distributions:

- *Data source.* For our calculations, we obtained data from the Shadowserver Foundation⁴, which has monitored the infection rates of the Gameover Zeus botnet and Conficker with respect to time. Gameover Zeus is a Peer 2 Peer botnet built by cyber criminals by sending emails with embedded malicious links or attachments, or enticing the victim to visit an infected website where a Trojan infected the victim. In comparison to the APT statistics,

³ Conficker was initially a computer worm, but when the payload was uploaded post-infection, it turned out as a Botnet

⁴Gameover Zeus <https://goz.shadowserver.org/stats/>

the information about botnet distribution relatively easy to gather from publicly available sources like Shadowserver, cause the anti-virus companies construct corresponding signatures shortly after the first discovery of botnet and starts logging occurrences.

- *Discussion of statistical approach.* Based on the available statistics collected over the months by Shadowserver, we ran a fitting test as described in Section 14.4. The results concluded that the most promising hypothesis about the probabilistic model is that data follow the (1) LOGNORMAL distribution. Therefore, it can be possible to predict the exact percentage of probability of the distribution of the botnet in some period in the future. From the other side, numerical methods for time series analysis can estimate the number of malware species in the wild after a defined period. The value of the last two methods is that the trends of the malware distributions can be predicted with better accuracy that just random guessing, cause human expert may fail to do it accurately.
- *Results - Applicability of statistical methods and possible failures for each risk.* We can state that (1) the available data follows LOGNORMAL distribution, so we can use these methods to say about future conditions. (2) That is not possible to fully rely on these methods since the uncertainty in the predictions is quite significant due to versatility in the data and tail sensitivity in the graph. However, the derived information can be used in qualitative ISRM since it is rather a set of fuzzy metrics.

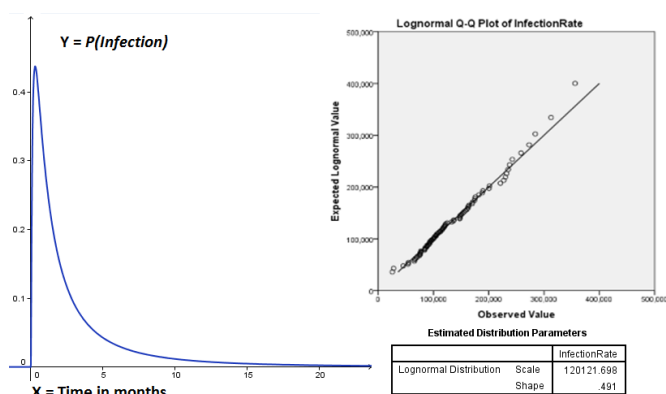


Figure 14.2: Gameover Zeus infection probability distribution and timeline. Right shows results of Q-Q plot of LogNormal distribution. Data source: The Shadowserver Foundation.

We ran the data points for Gameover Zeus in *QQ* plot and got the best fit with a Log-Normal curve with a tendency towards a thick tail, Fig. 14.2. Our results show that the Gameover Zeus botnet distribution is left-skewed (positive). The initial propagation speed is high (see Fig.14.4(b)), until saturation or patch released slows down the propagation, from which point the existing population deteriorates. In addition to adhering to epidemic propagation theory, there are several aspects that will influence the thickness of the tail. For example new versions of the malware being released, either exploiting a new vulnerability for increased propagation or changing behavior/coding to avoid scanners. In addition, we know that Conficker followed similar propagation and deterioration patterns, although Conficker⁵ was self-replicating [171]. According to our model: if the entity is vulnerable, the general probability of infection is 30% from the initial dissemination until the first month has passed. With a Mean population = 134,527, Standard Deviation = 64,797, and

⁵See also <http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker>

$\delta = 0.491$. The graph is sensitive to changes in the tails; this is also visible in the Q-Q plot results. The right tail of the graph in Fig. 14.2 would likely have been thicker if the data came from Conficker A+B, which remains active and deteriorating after six years.

- *Classification of Risk* - Single non-zero-day malware infections are generally detected and removed by antivirus software, and generally pose very little risk. However, dependent on the target infected and type of malware, the payoff can be complex. Self-propagating malware is usually more severe as they pose a threat to larger parts of the infected system. With some computer worms, the payoff can be considered simple, as the computer is infected (meaning non-operational) or not infected. Effectively having only two states of being. It is partially possible to predict exposure from such generic attacks, e.g. amount of vulnerable systems, but there is exposure to multi-vectored and other random effects which puts this risk in the *Third Quadrant*.

14.5.3 Distributed Denial of Service (DDoS) attacks

One of the most feared information attacks is the DDoS attacks, as they have the potential to break servers and deny access to a service to customers over an extended period causing massive revenue losses. By monitoring activity, we can obtain reliable numbers on how large the average DDoS attack is, and generate distributions of attack magnitudes. The answer to the RQ1 for DDoS:

- *Data source*. There is available open access statistics on DDOS attacks. So, we can use available statistics, yet it can not be fully relied on due to misleading detections or hardware malfunctions. Using numbers gathered from open access, we generated an example of possible distribution of DDOS occurrences for different bandwidth, shown in the Figure 14.3. Available threat intelligence indicated that the commonly observed DDoS magnitude at the time was between 0-90 Gbps, with distributions as seen in Table 14.1. Our test dataset corresponded to the numbers provided open access sources, having an arithmetic mean = 7.31, and Std. Dev = 13.55. The so-far largest reported DDoS attack was 500 Gbps, we can guesstimate that the generic probability of such an attack occurring annually is large; while the probability of such a large-scale directed attack at a single organization is negligible. There was no observed attack magnitudes over 90 Gbps in the surveys. However, we add such scenario A5 in Table 14.1.

Table 14.1: Example of DDoS attack magnitude distributions and probabilities, with conditional probabilities of semi-annual occurrence.

Scenario	Gbps	% of attacks	P(A B)
A1	<1	55.00 %	27.50%
A2	1-5	15.00 %	7.50%
A3	5-10	10.00 %	5.00%
A4	10-90	20.00 %	10.00%
A5	90+	Not observed (0.1%)	0.05%

- *Discussion of statistical approach*. There are several possible ways of approaching the statistical analysis of DDOS attacks. At first the probability of the DDOS attack can be calculated as simple (1) **CONDITIONAL PROBABILITY**, which gives an exact risk of being targeted for a DDOS attack out of possible attacks. Table 14.1 shows the results of calculations made for an organization that expects $P(B)=50\%$ annual chance of DDoS attack. At second, we can say something about the number of attacks and maximal used bandwidth by considering the historical information. However, the number of maximum reported DDOS attacks follow the (2) **EXPONENTIAL FUNCTION** and can not be predicted for the next years: $N = N_0 \cdot e^{t'}$ since some covert parameters are not taken into consideration like breakthrough network controller speed. At third, the particular scenario can be considered

14. ARTICLE VII - QUANTITATIVE RISK, STATISTICAL METHODS, AND THE FOUR QUADRANTS FOR INFORMATION SECURITY

when discretion intervals of DDOS bandwidth are considered like $P(DDOS > 90Gbps) = P(DDOS) \cdot P(> 90Gbps|DDOS)$. Also the (3) γ -DISTR. is the most applicable way of modeling such variety in scenarios.

- *Results - Uncertainty/ Confidence intervals.* The data and estimated parameters are valid only for some period until new attack methods emerge. However, it is still possible to form a corresponding γ -distribution to characterize the bandwidth for DDOS as it is depicted in the Figure 14.3, (a). So, corresponding CI can be extracted based on the parameters of the distribution to estimate the DDOS [48]. The Lower boundary can be neglected, however, exceeding the upper boundary may indicate that the parameters need to be re-evaluated for quantitative ISRM.

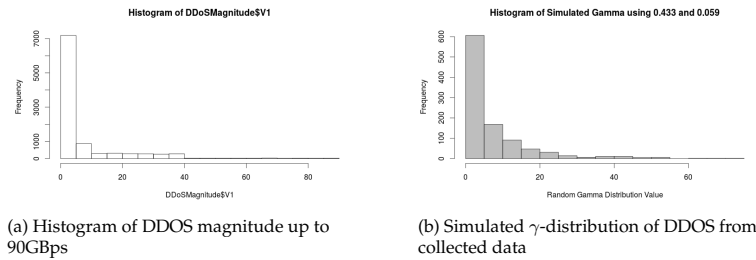


Figure 14.3: Comparison of the original DDOS data and modeled distribution

Though the data distribution can vary and, therefore, change the form depending on newly emerged technologies in network adapters industry, we can still use CI to estimate the boundary of the desired mitigation frame. It can be stated that the company wants to eliminate some % of the DDOS attacks and estimates the threshold of the attacks based on the previously collected information. The Table 14.2 presents an exact range of the bandwidth at which a particular % of the attacks can be mitigated. Our particular interest is the upper boundary of the CI since the lower boundary can be ignored at this point. For example, to withstand 95% of the DDOS attacks according to modeled γ -DIST. in the Fig. 14.3, (b) a company has to place a DDOS protection not lower than 62.82 Gpbs.

Table 14.2: Confidence Intervals for defined % of the DDOS attacks to be eliminated

To eliminate	50%	90%	95%	99%
Limit_lower, Gbps	0.531143	0.012634	0.002547	0.000061
Limit_upper, Gbps	9.411601	29.566104	39.241385	62.822911

- *Results - Applicability of statistical methods and possible failures for each risk.* We can estimate and put a threshold for an intrusion detection system to be capable of handling such attacks. Since it might be significant when guesstimating the risk that the organization takes when ignoring a particularly intensive attacks. For example, the network adapters increase capacity from 100Mbps up to 1Gbps over previous years. Therefore, the statistical models can be used for (1) DDOS bandwidth, and probability prediction and estimation, though constant failures of these models may indicate a need for re-evaluation of the maximal DDOS bandwidth. Furthermore, using the estimated probability, we can built also a qualitative risk estimators as more general linguistic characterization of the risk.
- *Classification of Risk* - As we have shown, it is possible to obtain distributions of DDoS attack magnitudes with associated probabilities. However, our observations can be offset by a single massive attack, such as Russia's DDOS attack on Estonia in 2007. This area is

also subject to Moore’s law, which means that historical observations of attack magnitudes will quickly become obsolete. We consider the payoff from DDoS attacks as simple; it either succeeds in denying service, or it does not while the duration of the attack determines the consequence. Our analysis, therefore, places risks of DDoS attacks in the *Third Quadrant*.

14.6 Discussion

Before presenting the Four Quadrant classification, we discuss issues that make information risks less predictable, which we have factored into our classification.

14.6.1 Factors leading into the Fourth Quadrant

- *The Complexity-Knowledge Gap* - Knowledge about system security quickly diminishes through the increase of *complexity* and *interconnectivity*, and the larger the system, the more uncertainty. Research on complex networks has demonstrated that the number of hosts on a network follows the power law [171], and our knowledge of risks in such systems and environments diminishes quickly. Audestad [26] calls this development the Complexity-Knowledge gap Fig. 14.4 (a).

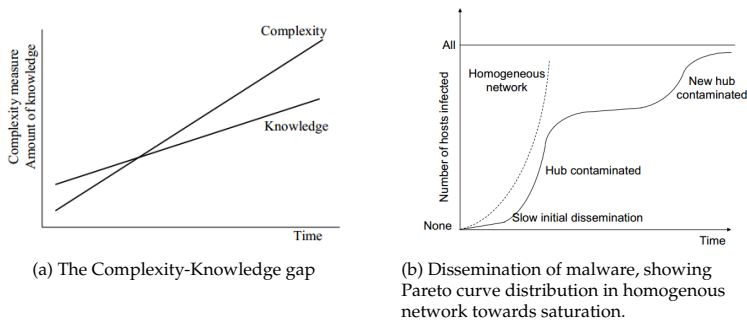


Figure 14.4: Factors leading into the Fourth Quadrant. *Pictures reprinted with permission, from Audestad, 2009 [26]*

- *Interconnection and Single Points of Failure (SPOF)* – While there is extensive knowledge of SPOF problems in the ICT domain, the risk posed by interconnectivity are easily overlooked and underestimated. For example, in a Banking incident from 2001 reported in [79], a human error triggered a SPOF at an operations company delivering ICT services to banks. This mistake caused a DoS for 114 banks and roughly one-fourth of the Norwegian population at the time. Such consequences would not have been possible without a large interconnected operations company representing a SPOF for much of the transactions in Norway. A centralization of operations and processes, which allows for the creation of one large strongly interconnected hub, in which the consequences of failure can become catastrophic for the system as a whole. The society and ICT have never been as interconnected at any period in the past, which quickly outdates most risk predictions based on historical data, as systems will find new ways to fail. The Complexity-Knowledge gap will also come into play, and we are likely to miss or overlook severe risks and potential consequences.
- *The Unpredictable Active Adversary* - In most cases, the activities that lead to a targeted attack are not visible, or they are negligible. The complexity of the extreme events such as cyberwarfare or cyberterrorism in the information security domain is so high that we can hardly notice it unless the damage is done, and the outcomes are obvious [102]. Since these

14. ARTICLE VII - QUANTITATIVE RISK, STATISTICAL METHODS, AND THE FOUR QUADRANTS FOR INFORMATION SECURITY

activities are well-planned and rather exceptional cases, there is a need for enormous data analytic and reconsideration of the Internet Crime like in the case with Stuxnet. For rare events, sophisticated classification/regression models have to be applied to conventional statistical methods to understand the nature of the event. It is sometimes necessary to get expert knowledge on the underlying adversary process rather than just rely on numbers for risk analysis. There is also the problem that the past will not reflect the future when it comes to resourceful and adaptable attackers. Advanced attackers will seek novel ways of achieving their objectives, which makes over-reliance on historical data dangerous.

- *Vulnerabilities to Cascading and Systemic risk in ICT* - Cascading and systemic risks are two types of high-level risks that are known to be large impact and low probability events. A cascading risk is when several components of a network fail in a cascade due to a crucial node going down, which subsequently causes an overload on the remaining nodes. Or when one component causes failure in interconnected components [79]. Whereas a systemic risk affects the global system and not just a particular entity. We define cascading risks as having the ability to cause localized harm, and systemic risks as having the capacity to cause global harm to a system. Of the latter, the Morris worm is probably the only known instance to have posed a systemic risk to all systems connected to the internet. The malware forced a segregation of the internet regions to prevent contamination and recontamination.

The consequences of a cascade can be devastating: In 2009, a Conficker infection within the Norwegian Police ICT systems reportedly caused damage ranging 30-50 million NOK and a downtime of 10 days. The Police computer system was largely homogenous, running older and vulnerable versions of Microsoft Windows, and Conficker was reported to have saturated at about 16 000 infections. Fig. 14.4 (b) shows general dissemination patterns of self-propagating malware; the stapled line indicates propagation in homogeneous networks. The distribution in the homogenous network follows exponential growth while the propagation in heterogeneous networks produces a model rather close to joint logistic function. Consequences from self-replicating malware and cascading risks are subject to fat tails, which requires caution when dealing with such phenomena.

14.6.1.1 The Four Quadrants Classification of Information Security Risk

Based on the case studies and the factors provided in the previous section, the non-exhaustive classification of information risks is presented in Fig. 14.5. This classification can help risk analyst in deciding whether to apply quantitative or qualitative risk analysis methods based on risk properties and where he can safely rely on statistical methods. The classification should not be used as an argument to not do risk assessments of Fourth Quadrant risks. However, we recommend avoiding long-term quantitative predictions with these risks due to their uncertain properties caused by a considerable complexity-knowledge gap. It is also possible that with more information and understanding, statistical risk analysis can move several of these risks out of the Fourth Quadrant.

14.7 Conclusion & Future work

In this paper we investigated quantitative risk calculations based on the available data. We provided a classification of where it is safe to apply statistical methods and where to expect a reasonable return on investment in improved decision making within the Four Quadrants. This work studied whether the statistical approaches are feasible to deal with Information Security Risks at all and what are the advantages of using such methods considering fact that they are purely reliable for the prediction. One can state that conventional statistical methods provides reliable accuracy only in case of significant amount of historical data and when the event in question is located within the tolerance interval from the past data. This article has presented several major cases within the Information Security

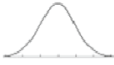
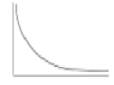
	1 Simple Payoff	2 Complex Payoff
A Mediocristan 	<i>First Quadrant, Extremely safe</i> 1. Hardware and component failure risks 2. Simple user errors 3. Exploiting known vulnerabilities from automated scans	<i>Second Quadrant, Safe</i> 1. Hardware system failure risks 2. Single Malware infections 3. Generic Phishing campaigns 4. Insider attacks 5. Known Targeted Attacks
E Extremistan 	<i>Third Quadrant, Safe</i> 1. DDoS Attacks 2. Self-propagating automated malware	<i>Fourth Quadrant, Black Swan Domain</i> 1. Cascading risks 2. Systemic risks 3. Novel APT / Targeted attacks 4. Terrorist attacks 5. Cyberterror/war 6. Complex Insider attacks (e.g. Snowden) 7. Complex User Errors

Figure 14.5: The Four Quadrants with Risk Classifications. *Based on Taleb[143]*

area, with a corresponding applicability study of statistical methods. We can conclude that there is a trade-off between the complexity of supplementary analytic and the risk's harm. It implies that trivial statistical methods are not suitable to deal with threat Intelligence in dangerous risks, yet general knowledge derived from such methods are reliable to make predictions better than random. Moreover, the statistical methods can not only be useful in quantitative analysis, yet also give a basis for qualitative measures. The observable outcomes may not always find a justification from the history since it might be some coincidence of logical triggers and human errors. Also, the implications of the study have discovered severe limitations of quantitative forecasts when it comes to targeted attacks, namely malicious individuals, and sophisticated threat agents. The increase in both complexity and interconnectivity limits our ability to forecast. It means that future advanced models such as Soft Computing should be considered to be able to expand the understanding of the covert malicious actions and make a better quantitative risk assessment.

Acknowledgments

The authors acknowledge Professors Jan Arild Audestad, Einar Snekkenes and Katrin Franke, and the data contributions made by the Shadowserver Foundation. The authors also recognize the sponsorship from COINS Research School for information security.

Article VIII - Cyber Security Risk Assessment of a DDoS Attack

Gaute Wangen, Andrii Shalaginov, & Christoffer Hallstensen
Cyber Security Risk Assessment of a DDoS Attack. International Conference on Information Security, 2016, Springer International Publishing, 183-202.

Abstract

This paper proposes a risk assessment process based on distinct classes and estimators, which we apply to a case study of a common communications security risk; a distributed denial of service attack (DDoS) attack. The risk assessment's novelty lies in the combination both the quantitative (statistics) and qualitative (subjective knowledge-based) aspects to model the attack and estimate the risk. The approach centers on estimations of assets, vulnerabilities, threats, controls, and associated outcomes in the event of a DDoS, together with a statistical analysis of the risk. Our main contribution is the process to combine the qualitative and quantitative estimation methods for cyber security risks, together with an insight into which technical details and variables to consider when risk assessing the DDoS amplification attack.

15.1 Introduction to InfoSec Risk Assessment

To conduct an information security (InfoSec) risk analysis (ISRA) is *to comprehend the nature of risk and to determine the level of risk* [11]. InfoSec risk comes from applying technology to information [36], where the risks revolve around securing the confidentiality, integrity, and availability of information. InfoSec risk management (ISRM) is the process of managing these risk while maximizing long-term profit in the presence of faults, conflicting incentives, and active adversaries [165]. Risks for information systems are mainly analyzed using a probabilistic risk analysis [15, 161], where risk is defined by estimations of consequence for the organization (e.g. financial loss if an incident occurred) and the probability of the risk occurring within a time interval. ISRA is mostly conducted using previous cases and historical data. Depending on statistical data (quantitative) alone for risk assessments will be too naive as the data quickly become obsolete [162] and is limited to only previously observed events [144]. While the subjective (qualitative) risk assessment is prone to several biases [89] (Part II) [144]. ISRM methods claim to be mainly quantitative [36, 62] or qualitative [46], but the quantitative versus qualitative risk situation is not strictly either-or. There are degrees of subjectivity and human-made assumptions in any risk assessment, and the intersection of these two approaches remains largely unexplored. The goal of this paper is to explore this intersection and discuss the benefits and drawbacks from each approach, and how they can complement each other. Moreover, we will discuss alternative ways of expressing uncertainty in risk assessment.

The remainder of the paper is structured as follows: The two following subsections introduces the reader to Distributed Denial of Service attacks and discusses the related work in ISRA. The Section 15.2 provides a brief description of the DDoS attack and development trend. Also, we present the method applied for ISRA and statistical analysis of the DDoS attack. Later in the Section 15.3 we give an insight into the qualitative ISRM approach

together with results and the quantitative risk assessment in the Section 15.4 based on statistical methods. Lastly, we discuss and conclude the results, the relationship between this work and previous ISRA work, limitations and propose future work in the Section 15.5.

15.1.1 Distributed Denial of Service Attacks

A denial of service (DoS) occurs when an ICT (Information and Communication Technology) resource becomes unavailable to its intended users. The attack scenario is to generate enough traffic to consume either all of the available bandwidth or to produce enough traffic on the server itself to prevent it from handling legitimate requests (resource exhaustion). The attacker needs to either exploit a vulnerable service protocol or to exploit network device(s) to generate traffic, or to amplify his requests via a server to consume all of the bandwidth. The DoS attack is distributed (DDoS) when the attacker manages to send traffic from multiple vulnerable devices. The attacker can achieve amplification through the exploitation of vulnerable protocols or through using botnets.

The increase of Internet throughput capacity has also facilitated the growth in traffic volume for DDoS-attacks. According to Arbor Networks, the largest observed attack in 2002 was less 1 Gbps (Gigabit per second). While the biggest observed attack until now targeted a British television channel and reportedly generated ≈ 600 Gbps of traffic. That is an approximate 60x development in capacity for DDoS attacks over the course of about 14 years, see Fig. 15.1.

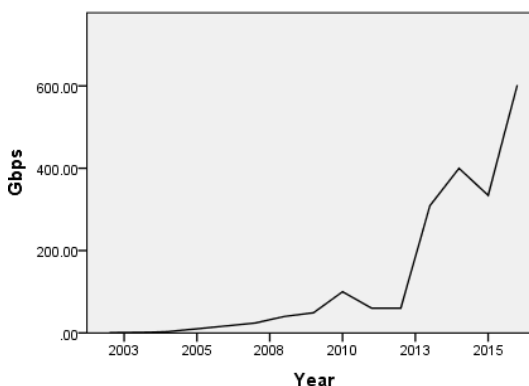


Figure 15.1: The development of bandwidth consumption (Gbps) of DDoS-attacks during the last 15 years. *Data source: Arbor Networks and media reports*

15.1.2 Related work in ISRA

The ISRA approach presented in this paper primarily builds on two previous studies; firstly, Wangen et.al.'s [161] Core Unified Risk Framework (CURF), which is a bottom-up classification of nine ISRA methods. The motivation behind CURF, was that there are several ISRA methods which conduct similar tasks, but there is no common way to conduct an ISRA. The approach ranked as most complete in CURF was ISO27005 [15] (from this moment referred to as ISO27005), while ISO27005 has many strengths, such as the process descriptions and taxonomies, one of the primary deficits of the ISO27005 is the lack of variables to consider and risk estimation techniques. The proposed approach in this paper builds on ISO27005 and addresses the outlined issues by defining classes and estimations for each step. Second, the probabilistic model presented in this paper builds on the feasibility study conducted by Wangen and Shalaginov [162], which discusses statistics and *Black*

Swan (see Taleb [144]) issues in ISRA. The Authors [162] found that there are Black Swan related aspects of the ICT domain that may render past observations (Statistics) inappropriate for probability, such as for novel and unique attacks, and the fast development of ICT, for example, Fig. 15.1. However, the authors also found that quantifying and modeling InfoSec risks have utility as long as the risk assessor is aware of the properties of the risk and the domain we are modeling. The Single and Annual Loss Expectancy (SLE/ALE) represent the most developed area of statistics in ISRA, where risk is described as the probability of a loss occurring [36]. Yet, risk must be considered as more than an expected loss [29]. Knowledge-based probabilities represent the main approach in ISRA [161], as previously discussed, there is utility in statistical data. The combination of these two approaches to probability has remained relatively unexplored in ISRA. So, this study proposes to combine a statistical and a qualitative ISRA to address the research gap.

Thus, this paper proposes a step-by-step process model for an ISRA of a distributed denial of service (DDoS) attack, and we apply the model to a real-world case as a proof of concept and feasibility study. The proposed ISRA approach is compliant with ISO27005.

15.2 Choice of Methods

This section outlines the core risk assessment concepts applied in this paper. First, we present the fundamentals of our risk analysis approach, then the qualitative ISRA method, and, lastly, discuss the statistical methods employed for quantitative analysis. Our overarching approach to validation is case study.

The proposed approach is based on the two ISO27005 steps (i)*Risk Identification -process of finding, recognizing and describing risks* [11], and (ii)*Risk Estimation - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable* [11]. We go further proposing classes and estimations for qualitative asset evaluation, and vulnerability, threat, and control assessment, together with both quantitative and qualitative risk estimations.

15.2.1 Fundamentals of risk analysis

Our proposed ISRA approach builds on the *set of triplets* as defined by Kaplan and Garrick [90], *Scenario, Likelihood, and Consequences*. In which we define the scenario as a combination of assets, vulnerability, threat, controls, and outcome. Each step in the approach generates useful knowledge in on its own, for example, a thorough threat assessment will provide information regarding opponents that are also useful in other risk-related activities and decision-making.

We combine the two approaches to risk and probability proposed by Aven [29]: (i) the frequentist (*"the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed"*), and (ii) the subjective knowledge-based probability (*"assessor's uncertainty (degree of belief) of the occurrence of an event"*). In terms of risk analysis, the key components of a risk (R) related to an activity for discussion and calculation are as follows [28] (p.229): R is described as a function of events (A), consequences (C), associated uncertainties (U), and probabilities (P). U and P calculations rely on background knowledge (K) which captures the qualitative aspect of the risk, for example, low K about a risk equals more U . Model sensitivities (S) display the underlying dependencies on the variation of the assumptions and conditions. Thus, $R = f(A, C, U, P, S, K)$ allows for a comprehensive output and incorporates the most common components of risk.

In the following section, we define the classes and estimators for each of the key elements of InfoSec risk as subjective knowledge, where the classes describe and categorize the risk components, and the estimators represent qualitative estimations based on expert knowledge and collected data. We do not define the scales for each estimator in this paper as this is individual for each organization.

15.2.2 Proposed Methodology for Qualitative Risk Analysis

The proposed qualitative methodology is based on descriptions, classes, and estimators. Based on ISO27005 we defined these for Assets evaluation, Vulnerability assessment, Threat assessment, and Control Assessment.

Asset identification and Evaluation.

To start, the Institution needs to identify and know its assets. We define *Asset Identification* as the process of identifying assets, while asset *Evaluation* assess their value, importance, and criticality. According to ISO27005[15] Annex B, there are two primary assets, (i) Business Processes & activities and (ii) Information. While *Asset Container* identifies where assets are stored, transported, and processed [46].

As a part of the process, we map the organizational goals and objectives for risk assessment, as these are important in deriving security goals for the InfoSec program. Also, we consider these when determining the risk event outcome.

- Assets - Something of value to the organization, person, or entity in question.
- Asset type - Description of the asset class, E.g. sensitive information.
- Asset Container - refers to where and how the asset is stored [46].
- Asset value - Estimated, either monetary or some intangible measurement of value
- Importance in Business Process is an estimation of the criticality of the asset in daily operations
- Asset criticality is the comprehensive assessment of the asset value and role in business process estimations.

Vulnerability Assessment

Vulnerability Identification is the process of identifying vulnerabilities of an asset or a control that can be exploited by a threat [11]. *Vulnerability Assessment* is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Vulnerabilities can be discovered through many activities, such as automated vulnerability scanning tools, security tests, security baselining, code reviews, and penetration testing. In the case of network penetration from a resourceful attacker, the analyst should also consider the *attacker graph*: how compromising one node in the network and establishing a foothold in the network can be exploited to move laterally inside the network and compromising additional nodes.

- Vulnerability type - A classification and description of vulnerability, *weakness of an asset or control that can be exploited by one or more threats* [11].
- Attack description - description of the attack for single attacks such as DDoS, or *attacker graph* where the adversary obtains access to an asset or asset group. The *attacker graph* is a visual representation of how the attacker traverses the network and gains access to an asset or a group of assets.
- Attack difficulty - Estimation, how difficult is it to launch the attack?
- Vulnerability severity - Estimation of the seriousness of the vulnerability
- System Resilience - How well will the system function under and after an assault, especially important for availability related risk
- Robustness - is the measure of how strong an attack will the system absorb.
- Exposure assessment - Determines exposure of entity's assets through the vulnerability and attack

Threat Identification and Assessment.

Threat identification is the process of identifying relevant threats for the organization. A Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization [11]. Besides mother nature, the threat is always considered as a human. For example, the threat is not the computer worm, but the worm's author. While the threat *Assessment* comprises of methods and approaches to determine the credibility and seriousness of a potential threat. The assessment process relies on the quality of threat intelligence and understanding of the adversary. For each threat, we propose to consider the following classes and estimators:

- Threat actor - Describes the human origin of the threat. There are several classes of threat agents in InfoSec, for example, malware authors, Cyberspies, and hackers.
- Intention - Defines what the threat actor's objectives with the attack, for example, unauthorized access, misuse, modify, deny access, sabotage, or disclosure.
- Motivation - Defines the primary motivation for launching the attack, previous work on malicious motivations [116] suggests Military or Intelligence, Political, Financial, Business, Grudge, Amusement, Self-assertion, Fun, and Carelessness.
- Breach type - which type of security breach is the threat actor looking to make; either confidentiality, integrity, availability, non-repudiation, or accountability.
- Capacity - Estimation of the resources he/she has at their disposal to launch the attack. For example, if an attack requires a lengthy campaign against your systems to succeed, the threat actor must have the resources available to launch such an attack.
- Capability - Estimation the threat's *know how and ability* for launching the attack.
- Willingness to attack - Estimation of how strong the motivation is to attack. For example, historical observations of the threat actor's frequency attacking the system is a good indicator.
- Threat severity is the comprehensive assessment of the above variables and the main output of the process.

Control Efficiency Estimation

Existing controls are measures already in place in the organization to modify risk [11]. *Control identification* is the activity of identifying existing controls for asset protection. *Control (efficiency) Assessment* are methods and approaches to determine how effectively the existing controls are at mitigating an identified risk.

The important issue to consider here is if the control sufficiently mitigates the risk in question. If the control is considered adequate, the risk can be documented for later review.

- Control Objectives - a written description or classification of what the control is in place to achieve.
- Control domain - Addresses in what domain the identified control is, either in the physical, technical, or administrative [68] (P.166-167).
- Control class - Addresses what the control is supposed to achieve; either prevent, detect, deter, correct, compensate or recovery [68] (P.166-167).
- Risk Event components - Consists of the *Asset Criticality, Exposure Assessment, and Threat Severity* for the identified risk event.
- Control efficiency - Estimation, addresses how efficient the control is at modifying the identified threat event and how well it achieves the control objectives.

15.2.3 Methodology for statistical risk analysis

The main statistical approaches considered in this paper are for theoretical analysis of the supplied historical data to run calculations. The motivation is to use conventional statistical methods to extract particular characteristics that are suitable for Quantitative ISRA. Additionally, we make hypotheses about an applicability of each particular method concerning available data. The calculations in this article are based on DDoS attacks data from the Akamai Technology's *State of the Internet* Reports (duration and magnitude) [19] and data gathered from the assessed case study institution on occurrence. These data are considered as quantitative observation of metrics of selected events, for example, some DDoS attacks over time. We utilize several community-accepted methods to deal with the historical data when it is necessary to make predictions in numbers. In particular, these are *Conditional Probability* and *Bayes Theorem*. First, the probabilistic model $p(x)$ is suggested and the corresponding set of parameters are estimated from the data to fit suggested distribution. In sequence, we apply statistical testing, which is an important part of our work since further for the DDoS case study we will justify the usage of a specific statistical method and make a hypothesis about their applicability. By testing, we can make a quantitative analysis of different statistical models quality. However, this is based only on pure analysis of the case's data and deducing the most applicable model that can describe the data and fit the purposes. The testing is suitable for determining whether the data follow a particular distribution model with some degree of defined beforehand confidence interval measured in %. The tests evaluate the actual observed data O with the expected data E from the hypothesized distribution. This is done with a help of QQ-PLOT or Quantile-Quantile plot representing a probability plot by depicting expected theoretical quantiles E and observed practical quantiles O against each other. The quality of hypothesized data distribution can be evaluated using linearity in this plot. It means that if the expectations match observations, even with some minor outliers, then the null hypothesis can be rejected, and data fit selected distribution. Second, the probabilistic model can be used to estimate the probability of similar events in this very period or later on. We observe the following well-known shortcomings of the probabilistic modeling. First, very few data points from history may cause a wrong decision. Second, very rare events have negligibly small probabilities which might cause trouble in predicting corresponding outcomes. The authors have applied the statistical analysis software IBM SPSS, GNU PSPP and RapidMiner. Later on, we also discuss the application of this methodology and possible ways of its improvement.

15.3 Case Study: Qualitative Risk Assessment of a DDoS attack

The case data together with relevant available statistics was collected from an institution whose IT-operations delivers services to about 3,000 users. The Case study Institution (hence referred to as "The Institution") is a high-availability organization delivering a range of services to the employees and users, mainly within research and development. The objectives of the IT-operations is to deliver reliable services with minimal downtime. The target of this study has a 10 Gbps main fiber optics connection link, which is the threshold of a successful DDoS attack. Fig. 15.2 displays the institution's network capacity and average traffic during regular weekdays, this case study considers attacks on the main link. During the five previous years, the Institution has had an average annual occurrence of two DDoS attempts, whereas none has been successful thus far. The goal of this assessment is to derive the qualitative risk of the Institution experiencing a successful attack by applying the proposed method.

The case study starts with asset identification and evaluation, further, considering vulnerabilities, threat assessment, control efficiency, and outcomes. Our contribution in this section is the application of the classes and qualitative estimators for each step of the risk assessment process.

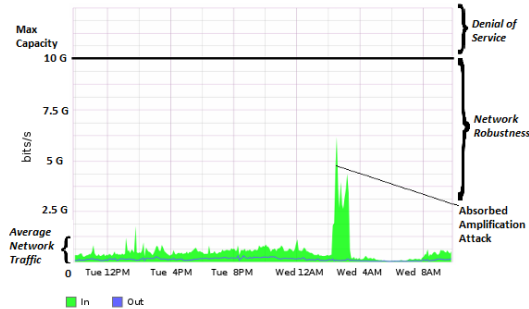


Figure 15.2: Illustration of Network robustness with an absorbed amplification attack. Network capacity at 10 Gbps, everything above constitutes a DoS.

Case Asset Evaluation. A DDoS attack is primarily an attack on the availability of the organization’s Internet connection. We compare the Internet connection capacity with a pipeline; it’s capacity limits the pipe’s throughput. Once the capacity is filled, no additional traffic can travel through the pipe. The attacker’s goal is to fill the pipeline with traffic and effectively block all legitimate traffic from traveling through the pipe. In the considered case, a successful DDoS attack will lock the users out of the network and prevent them from conducting their connectivity-dependent tasks. Most of the organization’s value chain is dependent on some level of connectivity, which makes the availability of services and assets the top priority when considering DDoS attacks. For simplicity, we consider "Service" as the main asset. As the institution is high availability and has up-time as one of the top priorities, service delivery is seen as crucial for production. Table 15.1 shows the classification and estimation considered for protection in the case study.

Table 15.1: Asset considerations for the DDoS attack

Asset type	Container	Protection Attribute	Importance in Business Process	Asset value	Asset Criticality
Service delivery	Infrastructure - Internet Pipeline	Availability	Essential (70-100)	Very high (50-85)	Essential (70-100)

Case Vulnerability Assessment Results. The Institution is exposed to several attack vectors for achieving DoS; for example resource starvation, application layer-based, and volumetric/flood. We provide a technical description of one attack, together with a vulnerability assessment. These estimations assume a 10 Gbps connection and the current security level in the Institution.

We measure the robustness in the DDoS-case in the gap between maximum network capacity and average traffic, illustrated in Fig. 15.2. A narrow gap between average load and maximum capacity is an indicator of fragility towards traffic generating attacks. To describe the network robustness we look at the maximum load versus the average load and measure the gap. The average load on the network is ≈ 1 Gbps; the system can absorb DDoS attacks up to ≈ 9 Gbps before the users experience denial of service, Fig. 15.2.

On resilience, the network will continue to function within acceptable service delivery up to traffic of about approximately 6-9 Gbps, depending on several variables such as weekday and hours, before users start to experience a degradation in service. Although attacks in this vicinity do not entirely cause a DoS, they reduce the latency in the network and efficiency of the workforce.

Based on our assessment of the network, we define four events (A) for further assessment:

15. ARTICLE VIII - CYBER SECURITY RISK ASSESSMENT OF A DDOS ATTACK

1. Attacks less than 6 Gbps which will be absorbed by the network robustness and will go by unnoticed by the users. (A1)
2. Attacks ranging 6-9 Gbps can cause reduction of service in the network. (A2)
3. Attacks ranging above 9 Gbps will cause DoS together with day-to-day use. (A3)
4. Attacks ranging from approximately 50 Gbps carry the potential for causing damage at the Internet Service Provider (ISP) level but carry the same consequences for the institution. (A4)

Attacks need to be able to generate a traffic within the ranges of scenarios A2 - A4 to be considered a threat potential threat in the case study, for illustration purposes, we only considered volumetric and flood-based attacks. The Institution's vulnerability is then the generic network capacity; we assume that no vulnerable services are running on the Institution's internal network. *Volumetric and flood based* attacks aims to saturate the amount of connections to the Link, through UDP (User Datagram Protocol) amplification generating a small amount of data from the attacker resulting in a lot of data traffic to the victim. UDP DDoS attacks exploit the fact that the UDP does not require a handshake to transmit data, and requires the service to return more bytes than the attacker sent with spoofed source IP. Hilden [76] provides the following example, *services running a vulnerable CharGen (Character generator protocol) can be exploited to generate traffic: the attacker sends a 1-byte sized packet with a spoofed IP (the target's IP) to the vulnerable servers. Due to no handshake, the servers immediately responds with a 1024 byte large packet to the target IP. The attacker can amplify his traffic (bytes sent) with 1024x (bytes received by the target) by exploiting one vulnerable server.* The Table 15.2 represents the attacker's bandwidth limits the attack.

The UDP amplification attack requires access to either a botnet or vulnerable service, both of which are readily available on the Internet, the former for hire and the latter for exploitation. The technical expertise required to launch an attack is low, where the trick is to locate vulnerable services through scans. The attacker can create traffic volumes in the ranges A2-A4, whereas attacks within ranges A2 and A3 are easily achieved with a low number of vulnerable services, Table 15.2. The A4 scenario requires more resources regarding bandwidth and services, but is still easily achieved for the technically skilled.

With a 10 Gbps connection, the Institution is inherently vulnerable to DDoS attacks, and since this is an attack on availability, the duration of the attack is also important to consider. We have defined the following downtime scenarios according to the Institution's risk tolerance:

1. Attack ranging between 0-10 min are considered negligible. (B1)
2. 11-30 min will produce a slight loss in production. (B2)
3. 31 - 120 min will produce a moderate loss in production, it is also likely that employees will seek out the helpdesk and cause extra overhead. (B3)
4. 2 - 24 hours will produce a critical loss in production, at this point everyone will have exhausted their tasks that can be solved without connectivity. (B4)
5. >24 hours will qualify as a catastrophe. (B5)

The Institution is exposed to volumetric and flood-based attacks due to ease of exploitation and effective amplification. Attacks ranging within A2-A3 are easily achievable with an initial technical insight, while ability to maintain the attack up to scenarios B3-B4 depend on a number of externalities that have a high level of uncertainty related to them, such as internal reaction time, threat capacity, and ISP capabilities. We address uncertainty related to the threat actor in the next section.

Table 15.2: Examples of approximate amplifications by exploiting vulnerable UDP, including possible amplification of the 100 Mbps connection. *Data source: Hilden [76], Norwegian Security Authority (NSM)*

Protocol	Amplification Ratio	100 Mbit/s ⇒
NTP	1:556	55.6 Gbit/s
CharGen	1:358	35.8 Gbit/s
QOTD	1:140	14 Gbit/s
Quake (servers)	1:63	6.3 Gbit/s
DNS (open resolver)	1:28-54	2.8 - 5.4 Gbit/s
SSDP	1:30	3 Gbit/s
SNMP	1:6	600 Mbit/s
Steam (Servers)	1:6	600 Mbit/s

Case Threat Assessment Results. Based on the exposure assessment, we identify and assess one threat actor in the position to trigger the attacks. For the threat actor, we consider the motivation, intention, willingness, capacity, and capability, to determine threat severity. The amplification attacks in question are easy to implement as long as vulnerable services are running, so, the analyst should consider less able attackers. However, for the case study we consider only one threat actor based on the estimated properties regarding the specifically analyzed DDoS attack:

Actor 1 is the politically motivated hacktivist whose weapon of choice is commonly the DDoS attack. Due to some of the research conducted in the Institution being controversial, they are the a potential target of Actor 1. We estimate the capacity for maintaining a lengthy attack (B3-B4) as *Moderate* and the capability for launching the attacks A2-A5 as *Very high*. It is uncertain whether this actor has been observed attacking their networks in the past, Table 15.3.

Table 15.3: Threat assessment for DDoS attack, K represents confidence in the estimates

Threat Actor	Motivation	Intention	Capacity	Capability	Willingness	K	Threat Severity
Actor 1	Political	Disruption	Moderate	Very high	Moderate	Low	High
Actor 2	Military or Intelligence	Access	Very high	Very high	Very low	Medium	Medium
Actor 3	Self-assertion	Deny Access	Low	Medium	Very high	High	Medium

Control Assessment Case Results. We provide a description of countermeasures for the considered attack, together with an estimation of efficiency which, for reactive controls, can be measured in time until the attack is mitigated.

In the case organization, the first and primary control strategy is to filter vulnerable UDP protocols on ingress network traffic. This control limits the attack surface of the organization's network and limits the effectiveness of exploiting vulnerable UDP based protocols. This control does not completely mitigate the possibility of attack because there is still network nodes that need to respond to UDP like Network Time Protocol and Domain Name System, but these are configured to provide low possibility for amplification values so that threat actors cannot effectively use them for attacking other systems on the Internet.

The second available mitigation strategy is to have a close cooperation with the Internet service provider's CSIRT. This control is vital because of the ISP's capabilities to blackhole (null-routing), rate-limit or even block network traffic that originates outside of their own network, or the country itself. For large DDoS attacks, the ISP is the only one capable of filtering away this traffic efficiently. On a day-to-day basis and within normal work hours, to involve the ISP CSIRT to start shaping or blocking traffic is highly effective and possible to implement within 1 to 2 hours. After working hours, 2 to 5 hours is estimated.

Table 15.4: Control efficiency estimation. K represents confidence in the estimates

Control Objectives	Control Domain	Control class	K	Control Efficiency
1. Filter UDP traffic	Logical	Preventive	Medium	Medium
2. Agreement with upstream ISP	Organizational	Reactive	High	High

15.3.1 Events and Results

The *Event outcomes* describes the range of outcomes of the event, consisting of asset, vulnerability, threat, and control, and how it affects the stakeholders and the organization. The process consists of identifying and describing the likely outcome(s) of the event regarding breaches of confidentiality, integrity, and availability, which does not entail calculations of consequence, as this is performed in the risk analysis. For example, an event outcome can have a financial impact or an impact on reputation.

The qualitative risk assessment shows that the most severe risk facing the organization is a DDoS campaign in the ranges A3-A4 (> 9 Gbps) and lasting longer than 2 hours (B4-B5). The Institution is currently vulnerable to such attacks due to the dependency on connectivity for running business processes. There is currently one politically motivated threat actor with a high capability of launching such an attack, but a moderate capacity for maintaining a lengthy campaign. We estimate the existing controls to be quite efficient to mitigate UDP amplification attacks, although the upstream ISP option includes third party dependencies which the institution does not control and introduces another layer of uncertainty. We continue the ISRA with the quantitative assessment of available real-case data from Akamai in the next section.

15.4 Quantitative Risk Analysis

The Risk analysis phase consists of estimating risk concerning $R = f(A, C, U, P, S, K)$. We assign the identified adverse outcomes, section 15.3.1, probability according to previous observations and subjective knowledge. A (event) is the result of the risk identification process and in the analysis described as a range of adverse outcomes based on the consequence calculations. There are primarily two approaches to probability, frequentist or subjective knowledge-based assessments (quantitative and qualitative). This section starts with the quantitative risk approach, before combining it with the qualitative results to obtain the risk.

15.4.1 Risk Calculations

The goal of the risk estimation is to reduce U related to risk occurring. For $P\&C$ calculations, we suggest merging the objective data gathered through observations and statistics with the subjective knowledge-based probabilities. We define the following:

- *Quantitative Assessment (Objective data)* - prior frequencies of occurrence, including past observations of the risk and generic risk data used to derive objective measurements of probability. Together with the gathering of relevant metadata through observations made by others.
- *Qualitative Assessment (Knowledge-based data)* - a combination of knowledge that is specific to the organization and the threat it is facing. Primarily derived from the *risk event components*, section 15.3.
- *Risk Estimate* - The final estimate of the probability for the risk, derived from quantitative and qualitative data.

The consequence estimation is derived primarily from two factors, monetary loss and intangible losses such as loss of reputation. Besides, the consequence estimation should consider the organizational objectives and goals [15]. The loss calculation is challenging as complex systems may fail in unpredictable ways. Possible data sources and input for consequence/impact considerations: prior loss data, monetary losses, consequences for organizational goals and objectives, and risk specific factors such as response time and attack duration.

Observed Frequencies of DDoS Attacks. By monitoring activity, we can obtain reliable numbers on how large the average DDoS attack and generate corresponding reports. The data applied in this article was provided by Akamai [19], and is based on 4,768 valid observations from 2014-2015, shown in the Tab. 15.5. There was no observed attack magnitudes over 255 Gbps in the data set. The observed frequencies of attacks towards the case study institution averaged two annual attacks during the last five years, $P_{occ} = \frac{1}{6} \approx 17\%$ of monthly occurrence, none of which have succeeded in attaining the necessary magnitude to achieve DoS. One of which managed to cause instability in the wireless network, thus, classifying as an A2 scenario.

Table 15.5: Frequencies of DDoS Magnitude observations from Akamai Dataset [19].

Characteristic	Valid	Missing	Mean	Median	Std. Dev.	Minimum	Maximum
Duration	4768	0	154,931.00	48,180.00	622,073.00	600	29,965,740.00
Gbps	4768	0	6.09	1.50	15.63	10^{-5}	249.00

Further, to test our hypothesis about the distribution of the data we used Q-Q plot, depicted in the Fig. 15.3. The plot shows the dependency between the observed data and expected data according to **Gamma distribution** prediction. Also, one can see two outliers at the high bandwidth interval indicating either unusual events or possible error in logging the characteristics of the events.

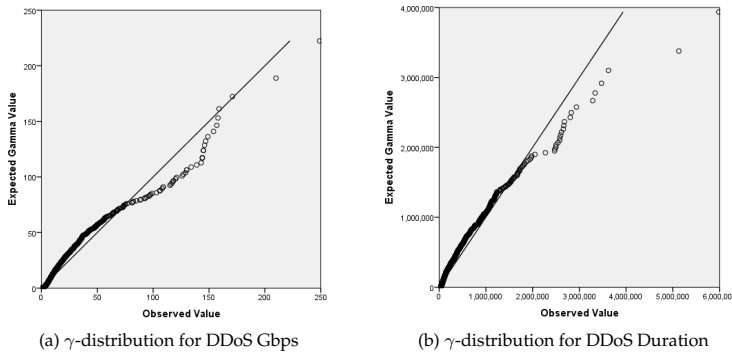


Figure 15.3: Fitting DDoS Magnitude and Duration data set by means of Q-Q Plot using γ -distribution. Two outliers are evident at the high end of the range for both distributions.

Observed values for Impact Estimation. By monitoring activity, we can also obtain reliable numbers on the duration of DDoS attacks and generate distributions. Our data provides us with Table 15.5, the data shows that the documented DDoS durations observed in this period were in the range from 600 up to $29 \cdot 10^6$ seconds, the longest lasting attack lasting approximately 347 days with magnitudes reaching about 4 Gbps. Removing two outliers from the data set gives a new mean value equal to $1.4 \cdot 10^5$ seconds. The Figure 15.4 displays the data clustering in the area around the mode and median. The majority of the data are distributed in this particular interval. In the case of probabilistic estimation,

it means that the data located far from this region are going to have a negligible level of occurrence.

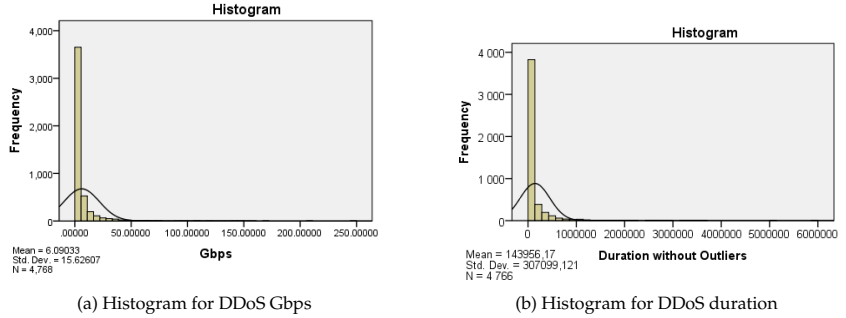


Figure 15.4: Histogram of DDoS magnitudes and durations with normal curve, without two largest outliers. *Data Source: Akamai [19]*

Our tests showed that there is no correlation between the variables "attack duration" and "attack magnitude". There is a small difference between the mean attack durations in the considered outcomes, but it is not statistically significant, Table 15.6. The A3 attacks seem to have shorter durations than the other; the one-way ANOVA (Analysis of variance model) shows that these two groups of observations are similar only to significance $P=85\%$. Yet, if we combine the A3 and A4 attacks this mean duration rises, and there is no significance.

Table 15.6: Frequencies for the defined events, *A*. *Data Source: Akamai [19]*

Scenario	Magnitude Gbps	Mean	Median	N	Std. Dev	% of attacks	$P(P_{occ} \wedge A)$
A1	<6	159,956.64	48,900	3,713	682,039.967	77.9	13.2%
A2	6 - 8.9	162,124.35	44,700	331	450,382.579	6.9	2.6%
A3	9 - 49.4	117,437.50	46,080	624	259,646.272	13.1	1.8%
A4	>49.5	178,485.20	52,380	100	284,012.424	2.1	0.4%

Fig. 15.5 depicts the correlation between duration and magnitude, where the attacks from the A1 and A2 scenarios are distributed nearly uniformly across the duration scale. It means that the nature of such attacks is more random and non-deterministic, which was also confirmed by our correlation tests. Going further, one can see that the majority of the attacks from the range of A3 are located in the duration range around $10^3 \dots 10^6$ seconds. Finally, same stands for the scenario A4, where the dispersion of possible magnitudes is large in comparison to A3. However, much higher frequency in case of probabilist model suppresses less frequent cases, while fuzzy logic describes data independently from the frequency of its appearance, only taking into consideration its possibility as described before by Shalaginov et.al. [125].

15.4.2 Probabilistic modeling for Risk Estimation

Unplanned downtime is an adverse event for which most ICT-dependent organizations need to have contingencies. The Institution considered in this paper have defined the severity metrics in Table 15.7, ranging from "Negligible" to "Catastrophe", together with the distribution of duration within the defined intervals. Losses are considered to be moderate up to two hours downtime, as most employees will be able to conduct tasks that do not require connectivity for a short period. Losses are estimated to start to accumulate after 2 hours of downtime. The analysis shows that the defined events B3-B5 are over 99%

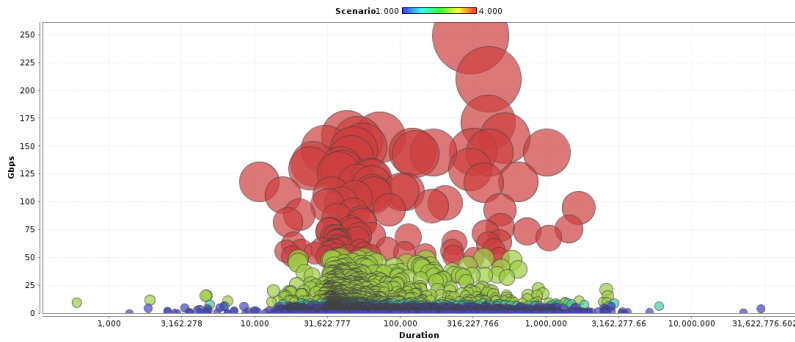


Figure 15.5: Bubble plot of the attack bandwidth depending on the duration for each scenario. Size of the bubble also denote magnitude of the attack. Scenarios are depicted with different colours.

likely to last more than 2 hours, which falls well outside of the Institutions risk tolerance. The conditional probability that the institution will suffer DDoS events in a given month is described in Table 15.6, right column. The risk estimation is modeled as an *Event tree*, Fig. 15.6, based on conditional probabilities $P(P_{occ} \wedge A \wedge B)$.

Table 15.7: Overview attack severity for the case study and duration frequencies. *Data Source: Akamai [19]*

Outcome	Interval (min)	Seconds	Severity	Frequency	% of Attacks
B1	0-10 min	0 - 600	Negligible	1	0.0
B2	11-30 min	601 - 1,800	Slight	1	0.0
B3	31 - 120 min	1,800 - 7,200	Moderate	28	0.6
B4	2 - 24 hours	7,201 - 86,400	Critical	3,346	70.2
B5	>24 hours	> 86400	Catastrophe	1,392	29.2

Sensitivity. The most sensitive numbers for the risk calculation is the P_{occ} , which is based on approximately ten observations from the last five years. The low amount of observations makes the mean sensitive to changes and one can capture this aspect in the analysis by assigning ranges to P_{occ} instead of concrete numbers. A probability range will help to make the assessment more robust, by for example adjusting for a range of 1-6 (or more) occurrences of DDoS attacks every year.

15.5 Discussion & Conclusion

In this section, we discuss the possibility of adjusting the risk model with additional qualitative input and propose an expanded model. We then discuss the limitations of the work and the potential future directions for the work.

15.5.1 Adjusting for Knowledge-based probability estimations

The primary objective of the ISRA process is to provide the decision-maker with as good a decision basis as possible. The benefit of the quantitative analysis is that the results are grounded in reality and defensible in a risk communication process. From the other side, the advantage of the qualitative risk assessment is that it allows more dynamic risk assessments. The main fragility of quantitative approaches is the dependence on the data quality

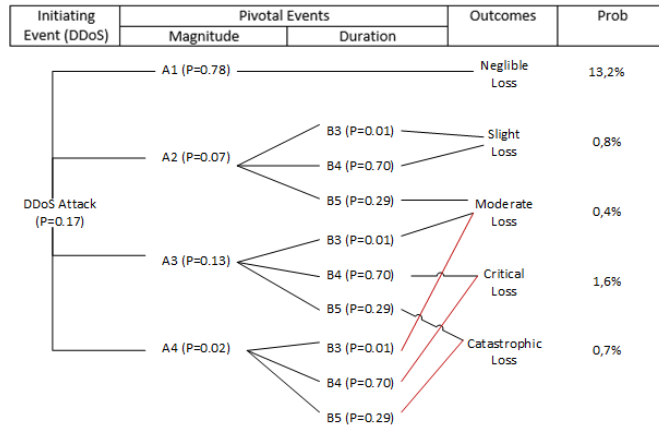


Figure 15.6: Event Tree displaying probability of monthly DDoS occurrence for the Case study.

and quantity of observations. We know about the fast-paced developments in ICT, for example, Fig. 15.1, showed the progress in capacity for DDoS attacks, and that attack trends may vary which have implications for the annual occurrence (discussed in [162]). The duration and magnitude of γ distributions should be more stable although the observed values are likely to increase according to the trend. However, the limitation of quantitative risk assessments is that attacks may not be present in the dataset, which makes the probabilistic approach less flexible as conducted in Section 15.4.2. It means that there is a need to have a control or introduce an additional factor that may indicate the possibility of the attacks.

One specific finding is the *Control efficiency*, Table 15.4, in which we have identified one proactive and one reactive control in place to mitigate an attack. For this discussion, we disregard the proactive control *Filter UDP traffic* as attacks have been occurring at a regular rate even with this control in place. We consider the reactive control, *Agreement with upstream ISP*, as a part of the risk assessment, where, during the workday we can expect an attack to be mitigated within 1-2 hours, and after working hours the handling time is between 2-5 hours. Although our quantitative analysis, Fig. 15.6, shows the combined risk of a monthly DDoS attack ranging from critical to a catastrophic loss at $\approx 2,3\%$. Further, if we include the control efficiency assessment we can adjust down the risk estimate for DDoS attacks lasting longer than two hours. A caveat here is that we must consider the event of control failure, in this case, we have a high degree of knowledge about the control efficiency and can put more trust in its functionality. However, third party dependency always comes with uncertainties due to information asymmetry problems between the service provider and the institution.

We also have the opportunity to adjust P_{occ} estimates based on the threat assessment, which applies to cases where the attacker attributes changes, for example, willingness to attack in the case of controversial political events. A thorough threat assessment is likely the best data source for more technical and rarer attacks than the DDoS. An understanding of the threat's intention and motivation will also provide a better understanding of possible consequences. The qualitative risk assessment shows that the Institution is facing one serious threat actor who both has the capacity, capability, and moderately willing to launch an attack. At the current time, the UDP-based amplification attack vector is easily exploitable and can generate traffic far beyond system limits to achieve all adverse scenarios between A2-A4. Which means that threat actors with less capacity and capability will be able to produce more powerful attacks. For a more technical and resource intensive

attack, it would make sense to consider the threat assessment where the more resourceful threats are linked to the more advanced attacks, for example, *Threat Actor 2* (Table 15.3) is more likely to be behind attacks in the critical to catastrophic loss events. *Actor 3* will be responsible for most attacks, but due to his limitations in capacity and capability; attacks will primarily be limited to short lasting and small magnitude attacks. While *Actor 2* is rarely observed, but can launch the catastrophic range attacks.

Taking into account both the threat and control assessments, we modify the Event tree to accommodate the qualitative assessment. For the combined assessment, we consider control efficiency concerning subjective ranges for *P* of a successful attack with Control 2 in place. To operationalize the threat assessment in the model, we have visualized our estimated attack ranges assigned to the identified threat actors in the left column, Fig. 15.7.

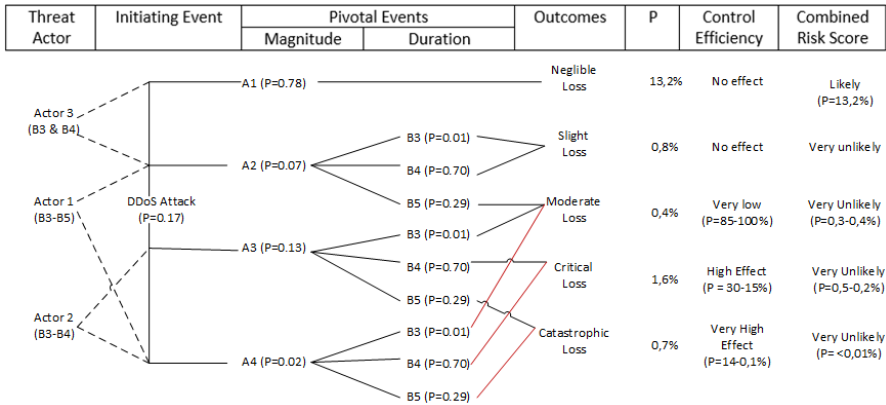


Figure 15.7: Expanded Event Tree also including subjective estimates of threat actors and control efficiency.

15.5.2 Limitations & Future Work

Our work has proposed an approach on how to combine quantitative and qualitative risk estimates. However, there is a limitation in our model due to the combination of the subjective and statistical assessments. We believe that application of possibilistic models such that Fuzzy Logic may help to understand the reasoning of statistical models better when the probabilities of two events are nearly equal and are very small. It means that the difference between two similar events can be below the limit of computing error because the event falls under the category of what Taleb defines as *Extremistan* (see [162, 143]). Therefore, applying a combination of subjective and objective estimators, we will be able to achieve better generalization of the model. Another way to improve the methodology is to use hierarchical models that ensemble inference of human-understandable Fuzzy Rules (also used for decision support) into a comprehensive framework.

We propose to apply our approach to model other cyber risks for further validation. The risk considered in this paper is a very technical communications risk, and the risk model would benefit from testing in areas where historical data is less available. Another limitation is the limited generalization of our case study; the ISRA approach should also be applied to other types of organizations

15.5.3 Conclusion

In this paper, we have proposed and applied classes and estimators for qualitative ISRA, which should contribute towards making the overall risk assessment process easier and more comprehensive. Our work shows that applying statistical methods for a cyber risk is feasible as long as there is data available. Moreover, with more accurate data there are possibilities for even more accurate and better quality models. Also, we adjusted the quantitative risk estimates with qualitative findings, for example, the definitions of scenario events (A and B) were based on qualitative measures of vulnerability and applied to categorize objective data. This paper also took the merging further by implementing the findings from the qualitative threat and control efficiency assessments into the probabilistic model. The control estimation is crucial to the risk estimation as it directly affects the estimation result, which in our case study made the most severe outcomes very unlikely. Thus, the conclusion is that combination of both the qualitative and quantitative aspects of ISRA is both feasible and beneficial. Defining an ISRM method as either-or in this manner may cause the risk analyst to miss out on valuable information for the assessment.

Acknowledgements

The authors acknowledge Professors Einar Snekkenes, Katrin Franke, and Dr. Roberto Ferreira Lopes from NTNU, Anders Einar Hilden from the Norwegian Security Authority (NSM), Karine Gourdon-Keller, David Fernandez, and Martin McKeay from Akamai. Also, the support from the COINS Research School for InfoSec is highly appreciated. Lastly, we acknowledge the contributions made by the anonymous reviewers.

Bibliography

- [1] The bpm methodology framework. <http://www.BPTrends.com>. Visited April 2014. xv, 37, 62, 67, 70, 71, 73
- [2] Inventory of risk assessment and risk management methods. Technical report, European Network and Information Security Agency (ENISA), 2006. 4, 13, 23, 52, 112, 114, 129
- [3] Methodology for evaluating usage and comparison of risk assessment and risk management items. Technical report, European Network and Information Security Agency (ENISA), 2007. 13, 114, 129
- [4] The risk it framework. Technical report, ISACA - Information Systems Audit and Control Association, 2009. 11, 32, 52, 55, 114, 118, 119, 122, 125
- [5] The risk it practitioner guide. Technical report, ISACA - Information Systems Audit and Control Association, 2009. 9
- [6] The risk it practitioner guide. Technical report, ISACA - Information Systems Audit and Control Association, 2009. 114, 117, 118, 119
- [7] Mehari 2010 - risk analysis and treatment guide, 2010. 11
- [8] Risk assessment of information systems (risikovurdering av informainformasjon). Technical report, The Norwegian Data Protection Authority (Datatilsynet), 2011. 32, 114, 116, 118, 119, 120, 122, 127
- [9] Risk taxonomy. Technical report, The Open Group, 2013. 11, 52, 53, 55
- [10] Information technology, security techniques, isms, overview and vocabulary, ISO/IEC 27000:2009. xiii, 27, 51, 52, 61, 64
- [11] Information technology, security techniques, isms, overview and vocabulary, ISO/IEC 27000:2014. xviii, 9, 10, 23, 91, 106, 134, 159, 161, 162, 163
- [12] Information technology, security techniques, isms, overview and vocabulary, ISO/IEC 27000:2016. 112, 118
- [13] Information technology - security techniques - information security management systems - requirements, ISO/IEC 27001:2013. 3, 9, 37, 62, 65, 69, 73
- [14] Information technology, security techniques, code of practice for information security management, ISO/IEC 27002:2013. 37, 62, 64, 65, 73, 75
- [15] Information technology, security techniques, information security risk management, ISO/IEC 27005:2011. xviii, 3, 4, 5, 10, 11, 12, 15, 32, 33, 51, 52, 55, 62, 64, 65, 69, 75, 78, 91, 92, 106, 112, 113, 118, 119, 120, 122, 133, 134, 136, 159, 160, 162, 169
- [16] Risk management - principles and guidelines, ISO/IEC 31000:2009. xviii, 9, 64

BIBLIOGRAPHY

- [17] Vivek Agrawal. A comparative study on information security risk analysis methods. *Journal of Computers*, 12(1):57–67, 2016. 4, 13, 23, 129
- [18] Ruth Sara Aguilar-Saven. Business process modelling: Review and framework. *International Journal of production economics*, 90(2):129–149, 2004. 66
- [19] Akamai. 2014-2015. Technical report, Akamai Technologies, 2015. xiii, xiv, xvi, 24, 35, 164, 169, 170, 171
- [20] Christopher J Alberts and Audrey J Dorofee. *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003. 58
- [21] Ross Anderson. Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pages 358–365. IEEE, 2001. 54
- [22] Louis Anthony Tony Cox. What’s wrong with risk matrices? *Risk analysis*, 28(2):497–512, 2008. 54
- [23] Philip S Anton, Robert H Anderson, Richard Mesic, and Michael Scheiern. The vulnerability assessment & mitigation methodology. Technical report, DTIC Document, 2003. 10
- [24] J.S. Armstrong. *Long-range Forecasting: From Crystal Ball to Computer*. A Wiley inter-science publication. John Wiley & Sons Canada, Limited, 1978. 148, 149
- [25] Yudistira Asnar and Fabio Massacci. A method for security governance, risk, and compliance (grc): a goal-process approach. In *Foundations of security analysis and design VI*, pages 152–184. Springer, 2011. 63
- [26] Jan A Audestad. *E-Bombs and E-Grenades: The Vulnerability of the Computerized Society*. Gjovik University College, 2011. xiv, 5, 11, 15, 20, 145, 148, 151, 155
- [27] Terje Aven. A semi-quantitative approach to risk analysis, as an alternative to gras. *Reliability Engineering & System Safety*, 93(6):790–797, 2008. 11
- [28] Terje Aven. *Misconceptions of risk*. John Wiley & Sons, 2011. xviii, 11, 115, 120, 146, 161
- [29] Terje Aven. The risk concept - historical and recent development trends. *Reliability Engineering & System Safety*, 99:33–44, 2012. xviii, 4, 11, 15, 17, 112, 115, 117, 120, 129, 161
- [30] Terje Aven. On the meaning of a black swan in a risk context. *Safety science*, 57:44–51, 2013. 20
- [31] Terje Aven. The concept of antifragility and its implications for the practice of risk analysis. *Risk Analysis*, 2014. 20
- [32] Terje Aven and Ortwin Renn. On risk defined as an event where the outcome is uncertain. *Journal of risk research*, 12(1):1–11, 2009. 112, 115, 120
- [33] Terje Aven, Willy Røed, and Hermann S Wiencke. *Risikoanalyse (Norwegian Ed)*. Prinsipper og metoder, med anvendelser. Oslo: Universitetsforlaget, 2008. xv, 10, 24, 104, 105
- [34] Behnia, Rashid, and Chaudry. A survey of information security risk analysis methods. *Smart Computing Review*, 2(1), 2012. 52

-
- [35] Vicki M. Bier. Challenges to the acceptance of probabilistic risk analysis. *Risk Analysis*, 19(4):703–710, 1999. 53, 57, 65
- [36] 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, 4, 5, 11, 20, 51, 53, 54, 56, 57, 58, 78, 85, 91, 106, 111, 112, 134, 159, 161
- [37] Rebecca M. Blank and Patrick D. Gallagher. Nist special publication 800-30, information security, guide for conduction risk assessments, revision 1, 2012. 5, 12, 14, 32, 113, 118, 119, 120, 125, 129
- [38] WG Bornman and L Labuschagne. A comparative framework for evaluating information security risk management methods. In *Information Security South Africa Conference, 2004*. 4, 13, 23, 52, 112, 114, 129
- [39] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3):523–548, 2010. 4, 14
- [40] Roger Burlton. *Business process management: profiting from process*. Pearson Education, 2001. xiii, 68, 73
- [41] Eric J Byres, Matthew Franz, and Darrin Miller. The use of attack trees in assessing vulnerabilities in scada systems. In *Proceedings of the international infrastructure survivability workshop, 2004*. 15
- [42] Harry Campbell. Risk assessment: subjective or objective? *Engineering Science and Education Journal*, 7(2):57–63, 1998. 5, 54, 56, 57
- [43] Katherine Campbell, Lawrence A Gordon, Martin P Loeb, and Lei Zhou. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448, 2003. 4, 14
- [44] Philip L. Campbell and Jason E. Stamp. *A classification scheme for risk assessment methods*. Sandia National Laboratories, 2004. 4, 13, 23, 52, 112, 114, 117, 128, 129, 134, 135
- [45] Richard A Caralli, Julia H Allen, and David W White. *CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience*. Addison-Wesley Professional, 2010. 63
- [46] Richard A Caralli, James F Stevens, Lisa R Young, and William R Wilson. Introducing octave allegro: Improving the information security risk assessment process. Technical report, DTIC Document, 2007. 5, 11, 12, 20, 32, 33, 113, 118, 119, 122, 124, 133, 135, 159, 162
- [47] Carlton M. Caves, Christopher A. Fuchs, and Rudiger Schack. Quantum probabilities as bayesian probabilities. *Phys. Rev. A*, 65:022305, 2002. 11
- [48] Charles J. Geyer. Stat 5102 notes: More on confidence intervals. <http://www.stat.umn.edu/geyer/old03/5102/notes/ci.pdf>, February 2003. accessed: 07.04.2015. 154
- [49] Thomas M Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid*, 2(4):741–749, 2011. 15

- [50] Gilbert A Churchill Jr. A paradigm for developing better measures of marketing constructs. *Journal of marketing research*, pages 64–73, 1979. 79, 93
- [51] Robert Damelio. *The basics of process mapping*. Taylor & Francis US, 2011. 61, 66
- [52] Folker Den Braber, Gyrd Brændeland, Heidi EI Dahl, I Engan, I Hogganvik, MS Lund, B Solhaug, K Stølen, and F Vraalsen. *The CORAS model-based method for security risk analysis*. SINTEF, Oslo, 2006. 12, 15, 32, 113, 119, 123
- [53] Folker den Braber, Ida Hogganvik, Mass Soldal Lund, Ketil Stølen, and Fredrik Vraalsen. Model-based security analysis in seven steps - a guided tour to the coras method. *BT Technology Journal*, 25(1):101–117, 2007. 5, 11, 12, 15
- [54] Arabin Kumar Dey and Debasis Kundu. Discriminating between the log-normal and log-logistic distributions. *Communications in Statistics-Theory and Methods*, 39(2):280–292, 2009. 149
- [55] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, pages 1–10, 2009. 52, 53, 58, 63
- [56] Andreas Ekelhart, Stefan Fenz, Markus Klemen, and Edgar Weippl. Security ontologies: Improving quantitative risk analysis. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 156a–156a. IEEE, 2007. 52, 55
- [57] S. Fenz and A. Ekelhart. Verification, validation, and evaluation in information security risk management. *Security Privacy, IEEE*, 9(2):58–65, 2011. 98, 102
- [58] Stefan Fenz, Johannes Heurix, Thomas Neubauer, and Fabian Pechstein. Current challenges in information security risk management. *Information Management & Computer Security*, 22(5):410–430, 2014. 4, 5, 13, 91, 92, 130
- [59] Bent Flyvbjerg. 'Case Study' in Norman K. Denzin and Yvonna S. Lincoln's *The Sage Handbook of Qualitative Research*. Thousan Oaks, CA, 2011. 22
- [60] International Organization for Standardization. Information technology - security techniques - information security management systems - requirements, ISO/IEC 27001:2005. 9
- [61] International Organization for Standardization. Information technology, security techniques, code of practice for information security management, ISO/IEC 27002:2005. 9
- [62] Jack Freund and Jack Jones. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, 2014. 5, 11, 12, 17, 20, 32, 43, 112, 113, 117, 118, 119, 123, 128, 131, 159
- [63] Roman Frigg and Stephan Hartmann. Models in science. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2012 edition, 2012. 22
- [64] Michael Gentile, Ron Collette, and Thomas D August. *The CISO Handbook: A Practical Guide to Securing Your Company*. Auerbach Publications, 2006. 9
- [65] Zoubin Ghahramani. Probabilistic modelling, machine learning, and the information revolution. In *presentation at MIT CSAIL*, 2012. 148
- [66] Barney G Glaser and Anselm L Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Aldine de Gruyter, 1967. 22

- [67] Shirley Gregor and Alan R Hevner. Positioning and presenting design science research for maximum impact. *MIS quarterly*, 37(2):337–355, 2013. 25, 40, 115
- [68] Peter H. Gregory. *All in one - CISA - Certified Information Systems Auditor - Exam Guide*. McGraw-Hill Companies, 2012. xiii, 5, 9, 15, 25, 55, 57, 63, 64, 65, 163
- [69] J. Hagen. Human relationships: A never-ending security education challenge? *Security Privacy, IEEE*, 7(4):65–67, 2009. 54
- [70] Paul Harmon et al. *Business process change: A guide for business managers and BPM and Six Sigma professionals*. Morgan Kaufmann, 2010. xv, 37, 61, 62, 66, 68, 70, 71, 72, 73, 75
- [71] Shon Harris. *All in one cissp. USA: MacGraw Hill*, 2013. 5, 17, 54, 56, 57, 58
- [72] Peter Herrmann and Gaby Herrmann. Security requirement analysis of business processes. *Electronic Commerce Research*, 6(3-4):305–335, 2006. 63
- [73] Joni Hersch. Smoking, seat belts, and other risky consumer decisions: Differences by gender and race. *Managerial and Decision Economics*, 17(5):471–481, 1996. 57
- [74] Alan Hevner and Samir Chatterjee. *Design research in information systems: theory and practice*, volume 22. Springer Science & Business Media, 2010. 22, 25, 114, 115
- [75] Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, 28(1):75–105, 2004. 22, 39, 114
- [76] Anders Einar Hilden. *UDP-Based DDoS Amplification Attacks*. Norwegian Security Authority (NSM), 2015. Lecture held at NTNU (Gjøvik), 07.10.2015. xvi, 166, 167
- [77] David Hilson. Extending the risk process to manage opportunities. *International Journal of Project Management*, 20(3):235–240, 2002. 55
- [78] Kjell J Hole. Management of hidden risks. *Computer*, 46(1):65–70, 2013. 20, 148
- [79] Kjell J Hole and L-H Netland. Toward risk assessment of large-impact and rare events. *Security & Privacy, IEEE*, 8(3):21–27, 2010. 20, 56, 128, 147, 155, 156
- [80] Douglas W Hubbard. *The failure of risk management: Why it's broken and how to fix it*. Wiley, 2009. 5, 14, 20, 51, 54, 55, 56, 57, 58
- [81] Douglas W Hubbard. *How to measure anything: finding the value of intangibles in business*. Wiley. com, 2010. 11
- [82] Douglas W Hubbard and Richard Seiersen. *How to measure anything in cybersecurity risk*. John Wiley & Sons, 2016. 5, 17, 18, 45
- [83] Stefan Jakoubi and Simon Tjoa. A reference model for risk-aware business process management. In *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on*, pages 82–89. IEEE, 2009. 62, 63
- [84] AK Jallow, B Majeed, K Vergidis, A Tiwari, and R Roy. Operational risk analysis in business processes. *BT Technology Journal*, 25(1):168–177, 2007. 63
- [85] Andrew Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Upper Saddle River, 2007. 51, 54, 55, 56, 58, 106
- [86] Allen C Johnston and Merrill Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pages 549–566, 2010. 4, 14

- [87] Jack Jones. An introduction to factor analysis of information risk (fair). *Norwich Journal of Information Assurance*, 2(1):67, 2006. 11, 32, 113, 119
- [88] Andrew Josey. *TOGAF Version 9: A Pocket Guide*. Van Haren Pub, 2009. 75
- [89] Daniel Kahneman. *Thinking, fast and slow*. Macmillan, 2011. 5, 11, 145, 159
- [90] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981. 10, 161
- [91] Max H Bazerman Katherine L Milkman, Dolly Chugh. How can decision making be improved? *Perspectives on Psychological Science*, 4(4):379–383, July 2009. 148
- [92] Kenneth J Knapp, Thomas E Marshall, R Kelly Rainer, and F Nelson Ford. Information security: management’s effect on culture and policy. *Information Management & Computer Security*, 14(1):24–36, 2006. 14
- [93] Ryan KL Ko. A computer scientist’s introductory guide to business process management (bpm). *Crossroads*, 15(4):4, 2009. 66
- [94] Ryan KL Ko, Stephen SG Lee, and Eng Wah Lee. Business process management (bpm) standards: a survey. *Business Process Management Journal*, 15(5):744–791, 2009. 66, 69
- [95] SA Kokolakis, AJ Demopoulos, and Evangelos A Kiountouzis. The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security*, 8(3):107–116, 2000. 63
- [96] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Foundations of attack–defense trees. In *Formal Aspects of Security and Trust*, pages 80–95. Springer, 2011. 12, 15
- [97] Andrew G Kotulic and Jan Guynes Clark. Why there aren’t more information security research studies. *Information & Management*, 41(5):597–607, 2004. 4, 14, 54, 57, 58, 62, 70, 78, 92
- [98] Bill Kuechler and Vijay Vaishnavi. On theory development in design science research: anatomy of a research project. *European Journal of Information Systems*, 17(5):489–504, 2008. 22
- [99] Douglas J Landoll. *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2005. 55, 57
- [100] Paul D. Leedy and Jeanne Ellis Omrod. *Practical Research - Planning and Design*. Pearson Educational International, 2010. 21, 22
- [101] Aleksandr Lenin, Jan Willemson, and Dyan Permata Sari. Attacker profiling in quantitative security assessment based on attack trees. In *Nordic Conference on Secure IT Systems*, pages 199–212. Springer, 2014. 15
- [102] James Andrew Lewis. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Technical report, Center for strategic & international studies, 2002. 155
- [103] Gary Locke and Patrick Gallagher. 800-39 nist sp, managing information security risks - organization, mission, and information systems view. Technical report, National Institute of Standards and Technology: U.S. Department of Commerce, 2008. xv, 12, 37, 62, 64, 70, 71, 72, 95
- [104] George F Loewenstein, Elke U Weber, Christopher K Hsee, and Ned Welch. Risk as feelings. *Psychological bulletin*, 127(2):267, 2001. 57, 102

- [105] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. Risk analysis of changing and evolving systems using coras. In *Foundations of security analysis and design VI*, pages 231–274. Springer, 2011. 32, 113, 117, 119
- [106] Artie Mahal. *How Work Gets Done: Business Process Management, Basics and Beyond*. Technics Publications, LLC, 2010. xiii, xv, 37, 61, 62, 66, 67, 68, 70, 71, 72, 73, 75
- [107] Salvatore T March and Gerald F Smith. Design and natural science research on information technology. *Decision support systems*, 15(4):251–266, 1995. 22
- [108] Sjouke Mauw and Martijn Oostdijk. Foundations of attack trees. In *International Conference on Information Security and Cryptology*, pages 186–198. Springer, 2005. 15
- [109] Nicholas Metropolis and Stanislaw Ulam. The monte carlo method. *Journal of the American statistical association*, 44(247):335–341, 1949. 11
- [110] Nikola Milanovic, Bratislav Milic, and Miroslaw Malek. Modeling business process availability. In *Services-Part I, 2008. IEEE Congress on*, pages 315–321. IEEE, 2008. 63
- [111] R. Moen and C. Norman. *Evolution of the PDCA Cycle*. Associates in Process Improvement, 2011. 69
- [112] Ramon E. Moore. *Introduction to Interval Analysis*. SIAM, 1966. 11
- [113] NSM. Veiledning i risiko- og sårbarhetsanalyse (guidelines for risk and vulnerability assessments). Technical report, Nasjonal Sikkerhetsmyndighet (Norwegian National Security Authority), 2006. 12, 32, 33, 43, 113, 119, 128, 131, 133, 135
- [114] Hilarie Orman. The morris worm: a fifteen-year perspective. *IEEE Security & Privacy*, 1(5):35–43, 2003. 18
- [115] Sevgi Ozkan and Bilge Karabacak. Collaborative risk method for information security management practices: A case context within turkey. *International Journal of Information Management*, 30(6):567–572, 2010. 4, 53, 55, 56, 57, 63, 75
- [116] Donald L. Pipkin. *Halting the Hacker: A Practical Guide to Computer Security, Second Edition*. Pearson Education, 2003. 163
- [117] Lisa Rajbhandari. *Risk Analysis Using "Conflicting Incentives" as an alternative notion of Risk*. PhD thesis, Gjøvik University College, 2013. 12, 15, 32, 113, 117, 118, 120, 122
- [118] Lisa Rajbhandari and Einar Snekkenes. Using the conflicting incentives risk analysis method. In *Security and Privacy Protection in Information Processing Systems*, pages 315–329. Springer, 2013. 119
- [119] Lisa Rajbhandari and Einar Arthur Snekkenes. Case study role play for risk analysis research and training. In *Proceedings of the 10th International Workshop on Security in Information Systems - Volume 1: WOSIS, (ICEIS 2013)*, pages 12–23, 2013. 44
- [120] Wanda Roos and Rene Van Eeden. The relationship between employee motivation, job satisfaction and corporate culture: empirical research. *SA journal of industrial psychology*, 34(1):54–63, 2008. 14
- [121] Vineet Saini, Qiang Duan, and Vamsi Paruchuri. Threat modeling using attack trees. *Journal of Computing Sciences in Colleges*, 23(4):124–131, 2008. 15
- [122] Mark NK Saunders, Mark Saunders, Philip Lewis, and Adrian Thornhill. *Research Methods For Business Students, 5/e*. Pearson Education India, 2011. 21

- [123] Stuart Edward Schechter. *Computer security strength & risk: A quantitative approach*. PhD thesis, Citeseer, 2004. 12, 17, 57, 58
- [124] Bruce Schneier. Attack trees. *Dr. Dobbi's journal*, 24(12):21–29, 1999. 11, 12, 15
- [125] Andrii Shalaginov and Katrin Franke. A new method of fuzzy patches construction in neuro-fuzzy for malware detection. In *IFSA-EUSFLAT*. Atlantis Press, 2015. 170
- [126] Palaniappan Shamala, Rabiah Ahmad, and Mariana Yusoff. A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications*, 18(1):45–52, 2013. 4, 13, 23, 112, 114, 129, 133, 134
- [127] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. Taxonomy of information security risk assessment (isra). *Computers & Security*, 57:14–30, 2016. 3, 4, 14, 16, 23, 24, 43, 44, 112, 114, 116, 129, 133, 134
- [128] James Shanteau and Thomas R. Stewart. Why study expert decision making? some historical perspectives and comments. *Organizational Behavior and Human Decision Processes*, 53(2), 1992. 5, 57
- [129] Piya Shedden, Wally Smith, and Atif Ahmad. Information security risk assessment: towards a business practice perspective. In *Australian Information Security Management Conference*. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2010. 54, 56
- [130] Mikko T Siponen and Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *ACM Sigmis Database*, 38(1):60–80, 2007. 4, 5, 11, 53
- [131] Paul Slovic. Perception of risk. *Science*, 236(4799):280–285, 1987. 5, 57
- [132] Paul Slovic, Melissa L Finucane, Ellen Peters, and Donald G MacGregor. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis*, 24(2):311–322, 2004. 5, 57
- [133] Einar Snekkenes. An information security risk management research menu. *Norsk informasjonssikkerhetskonferanse (NISK)*, 2012. 4, 5, 11, 14, 52, 57
- [134] Einar Snekkenes. Position paper: Privacy risk analysis is about understanding conflicting incentives. In Simone Fischer-Haubner, Elisabeth Leeuw, and Chris Mitchell, editors, *Policies and Research in Identity Management*, volume 396 of *IFIP Advances in Information and Communication Technology*, pages 100–103. Springer Berlin Heidelberg, 2013. 113
- [135] Teodor Sommestad, Mathias Ekstedt, and Hannes Holm. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, 7(3):363–373, 2013. 16
- [136] Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson. Cyber security risks assessment with bayesian defense graphs and architectural models. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–10. IEEE, 2009. 15
- [137] Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson. A probabilistic relational model for security risk analysis. *Computers & Security*, 29(6):659–679, 2010. 16
- [138] Wes Sonnenreich, Jason Albanese, and Bruce Stout. Return on security investment (rosi)-a practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1):45–56, 2006. 17

- [139] Janine L Spears and Henri Barki. User participation in information systems security risk management. *MIS quarterly*, pages 503–522, 2010. 14
- [140] Greg Stone and Pierre Noel. Cloud risk decision framework. Technical report, 2012. 32, 114, 116, 117, 119, 120, 126, 127
- [141] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Nist 800-30, risk management guide for information technology systems, special publication, 2002. 63, 65
- [142] Amril Syalim, Yoshiki Hori, Kouchi, and Kouchi Sakurai. Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft’s security management guide. *International Conference on Availability, Reliability and Security*, pages 726–731, 2009. 4, 13, 23, 52, 112, 114, 129
- [143] Nassim Nicholas Taleb. Errors, robustness, and the fourth quadrant. *International Journal of Forecasting*, 25(4):744–759, 2009. xiii, xiv, 18, 19, 24, 34, 35, 39, 40, 44, 146, 147, 148, 157, 173
- [144] Nassim Nicholas Taleb. *The Black Swan: The Impact of the Highly Improbable*. Random House LLC, 2nd ed. edition, 2010. 5, 11, 17, 18, 24, 34, 39, 44, 102, 104, 112, 128, 145, 146, 147, 148, 159, 161
- [145] Nassim Nicholas Taleb. *Antifragile: things that gain from disorder*. Random House LLC, 2012. 104
- [146] Stefan Taubenberger and Jan Jürjens. It security risk analysis based on business process models enhanced with security requirements. In *Modeling Security Workshop, Toulouse, France, 2008*. 63
- [147] David J Teece. Capturing value from knowledge assets: The new economy, markets for know-how, and intangible assets. *California management review*, 40(3), 1998. 75
- [148] Carrison KS Tong, KH Fung, Henry YH Huang, and Kwok Kwan Chan. Implementation of iso17799 and bs7799 in picture archiving and communication system: local experience in implementation of bs7799 standard. In *International Congress Series*, volume 1256, pages 311–318. Elsevier, 2003. 57
- [149] Henrik Miguel Nacarino Torres, Niclas Hellesen A, and Erlend Lundsvoll Brækken. Bruk av rotårsaksanalyse i informasjonssikkerhet. B.S. thesis, NTNU in Gjøvik, 2016. xiii, 16
- [150] Amos Tversky, D Kahneman, and Rational Choice. The framing of decisions. *Science*, 211:453–458, 1981. 57
- [151] Amos Tversky and Daniel Kahneman. Judgment under uncertainty: Heuristics and biases. In Dirk Wendt and Charles Vlek, editors, *Utility, Probability, and Human Decision Making*, volume 11 of *Theory and Decision Library*, pages 141–162. Springer Netherlands, 1975. 57
- [152] Wil MP van der Aalst. Business process management: A comprehensive survey. *ISRN Software Engineering*, 2013, 2013. 61, 66
- [153] Wil MP Van Der Aalst, Arthur HM Ter Hofstede, and Mathias Weske. Business process management: A survey. In *Business process management*, pages 1–12. Springer, 2003. 66
- [154] 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. 79

- [155] Basie Von Solms and Rossouw Von Solms. The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376, 2004. 3, 51, 55
- [156] Gaute Wangen. Conflicting incentives risk analysis: A case study of the normative peer review process. *Administrative Sciences*, 5(3):125, 2015. 7, 122
- [157] Gaute Wangen. An initial insight into infosec risk management practices. In *Proceeding of Norwegian Information Security Conference / Norsk informasjonssikkerhetskonferanse - NISK 2015 - Ålesund*, volume 2015. Open Journal Systems, 2015. ix, 7, 30, 37, 39, 40, 45, 89, 91, 92, 115, 118, 126
- [158] Gaute Wangen. The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information*, 6(2):183–211, 2015. 7
- [159] Gaute Wangen. An initial insight into information security risk assessment practices. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, volume 8 of *Annals of Computer Science and Information Systems*, pages 999–1008. IEEE, 2016. ix, 7, 30, 37, 39, 40, 45, 142
- [160] Gaute Wangen. Information security risk assessment: A method comparison. *Computer*, 50(4):52–61, 2017. ix, 7, 33, 38, 39, 40, 43
- [161] Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness - core unified risk framework. In *Under Review. ...*, 2017. ix, 3, 7, 31, 38, 39, 40, 105, 133, 134, 135, 136, 159, 160, 161
- [162] Gaute Wangen and Andrii Shalaginov. *Risks and Security of Internet and Systems: 10th International Conference, CRiSiS 2015, Mytilene, Lesbos Island, Greece, July 20–22, 2015, Revised Selected Papers*, chapter Quantitative Risk, Statistical Methods and the Four Quadrants for Information Security, pages 127–143. Springer International Publishing, Cham, 2016. ix, 7, 24, 34, 39, 40, 85, 102, 118, 128, 159, 160, 161, 172, 173
- [163] Gaute Wangen, Andrii Shalaginov, and Christoffer Hallstensen. Cyber security risk assessment of a ddos attack. In *International Conference on Information Security*, pages 183–202. Springer, 2016. ix, 7, 24, 34, 35, 39, 40, 41
- [164] 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. ix, 7, 27, 37, 39, 40, 47, 65, 73, 77, 78, 80, 82, 86, 87, 91, 92, 98, 99, 102, 118, 126, 130, 133, 142, 145
- [165] Gaute Wangen and Einar Arthur Snekkenes. A comparison between business process management and information security management. In M. Paprzycki M. Ganzha, L. Maciaszek, editor, *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, volume 2 of *Annals of Computer Science and Information Systems*, pages 901–910. IEEE, 2014. ix, 7, 29, 37, 39, 40, 45, 47, 159
- [166] Branimir Wetzstein, Zhilei Ma, Agata Filipowska, Monika Kaczmarek, Sami Bhiri, Silvestre Losada, Jose-Manuel Lopez-Cob, and Laurent Cicurel. Semantic business process management: A lifecycle based requirements analysis. In *SBPM*, 2007. 66
- [167] H.J. Whitman, M.E. & Mattord. *Roadmap to information Security: For IT and InfoSec Managers*. Cengage Learning, 2011. 9, 51
- [168] Michael E Whitman and Herbert J Mattord. *Management of information security*. CengageBrain.com, 2010. 9

- [169] John Wunder, Adam Halbardier, and David Waltermire. *Specification for Asset Identification 1.1*. NIST - US Department of Commerce, National Institute of Standards and Technology, 2011. 65, 75
- [170] Zeki Yazar. A qualitative risk analysis and management tool-cramm. *SANS InfoSec Reading Room White Paper*, 2002. 11, 12, 32, 112, 113, 118, 119, 122
- [171] Shui Yu, Guofei Gu, Ahmed Barnawi, Song Guo, and Ivan Stojmenovic. Malware propagation in large-scale networks. *IEEE Transactions on Knowledge & Data Engineering*, (1):170–179, 2015. 151, 152, 155
- [172] Claudia Zeisberger and David Munro. *"The 4 Quadrants": A World of Risk and a Road Map to understand It*. INSEAD, 2010. 20
- [173] Yu Zhiwei and Ji Zhongyuan. A survey on the evolution of risk evaluation for information systems security. *Energy Procedia*, 17:1288–1294, 2012. 55, 56, 99
- [174] Martijn Zoet, Richard Welke, Johan Versendaal, and Pascal Ravesteyn. Aligning risk management and compliance considerations with business process development. In *E-Commerce and Web Technologies*, pages 157–168. Springer, 2009. 63

