

IMPROVING THE Maturity OF BUSINESS INFORMATION SECURITY

Y. Bobbert

On the Design and Engineering of a
Business Information Security Artefact



The research reported in this thesis was conducted at the Institute for Computing and Information Sciences of Radboud University Nijmegen in partnership with University of Antwerp, under the auspices of the Enterprise Engineering Network.

EE-Network dissertation series: 2018-1

Published and distributed by: Datawyse | Universitaire Pers Maastricht

Keywords: Information Security, Risk Management, Collaboration, Business Management, Knowledge management, Information Security Governance, Group Support System Research, Delphi Research, Design Science Research, Design Thinking

ISBN: 978 94 6295 973 6

Availability: Publicly available via <http://repository.ubn.ru.nl/> and <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

Copyright © by Yuri Bobbert

All rights reserved. No part of this publication may be reproduced, stored in a retrieval database or published in any form or by any means, electronic, mechanical or photocopying, recording or otherwise, without the prior written permission of the author Yuri Bobbert.

RADBOUD UNIVERSITY NIJMEGEN

IMPROVING THE MATURITY OF BUSINESS INFORMATION SECURITY

PROEFSCHRIFT

ter verkrijging van de **graad van doctor**
aan de Radboud Universiteit Nijmegen
op gezag van de rector magnificus prof. dr. J. H. J. M. van Krieken,
volgens besluit van het college van decanen

én

ter verkrijging van de **graad van doctor**
in de Toegepaste Economische Wetenschappen
aan de Universiteit Antwerpen
op gezag van de rector magnificus prof. dr. H. Van Goethem.
in het openbaar te verdedigen op maandag 2 juli 2018
om 16.30 uur precies

door

Yuri Bobbert
geboren 28 november 1973
te Soest

Promotoren:	Prof. dr. H. A. Proper	
	Prof. dr. S. De Haes	Universiteit Antwerpen, België
	Prof. dr. J.B.F. Mulder	Universiteit Antwerpen, België
Manuscriptcommissie:	Prof. dr. F. W. Vaandrager	Chair
	Prof. dr. E. R. Verheul	
	Prof. dr. R. J. Wieringa	Universiteit Twente
	Prof. dr. J. Verelst	Universiteit Antwerpen, België
	Dr. W. Hafkamp	Rabobank

CONTENTS	5
LIST OF FIGURES & TABLES	12
INSPIRATION	20
1. INTRODUCTION	24
1.1 Motivation based on personal observations	25
1.2 Motivation based on literature	26
1.3 Problem statement	31
1.4 Research questions, objectives and deliverables	34
1.5 Thesis structure	37
2. RESEARCH APPROACH	43
2.1 Introduction	43
2.2 Selecting research methods	44
2.2.1 Quantitative & qualitative research	44
2.2.2 Ontological aspects of research	47
2.2.3 Epistemological aspects of research	48
2.2.4 Tacit knowledge	49
2.2.5 Explicit knowledge	49
2.3 Relevant research methods for BIS research	50
2.3.1 Literature research	50
2.3.2 The Delphi research method	53
2.3.3 Group Support System research	55
2.3.4 Case study research	58
2.3.5 Design Science Research strategy	61
2.3.6 Using Design Science Research to create artefacts	64
2.3.7 Relevant methods and techniques for this research project	66
2.4 Proposed multi-method approach	68
2.5 Research assumptions	70

3.	DEFINING KEY CONCEPTS OF BUSINESS INFORMATION SECURITY	76
3.1	Introduction	77
3.1.1	Information risk and security management	80
3.1.2	Business Information Security maturity & alignment	86
3.1.3	Continuous improvement	86
3.1.4	Strategic planning	88
3.1.5	Information Security as a Strategic Unique Selling Point	89
3.1.6	Governance of Business Information Security	90
3.1.7	Interventions & practices	92
3.1.8	Structures, processes and relational mechanisms	94
3.1.9	Requirements	95
3.2	Conclusion	97
4.	EXPLORING MANAGEMENT INTERVENTIONS	98
4.1	Introduction	99
4.2	Defining the mid-market as a research area	99
4.3	Problems for mid-market organisations	101
4.4	Research approach for exploring management interventions	102
4.4.1	Considerations for the selection of interventions	104
4.4.2	Selecting the source of intervention candidates	108
4.4.3	ISO as a frame of reference for BIS interventions	109
4.4.4	Expert panel research for the selection of mid-market interventions	112
4.4.5	Scoring of interventions on Ease of implementation and Effectiveness	114
4.4.6	Final selection of BIS interventions	115
4.4.7	Main barriers for MBIS according to the experts	115
4.4.8	Expert panel data analysis	116
4.4.9	Relevant interventions	118
4.5	Performing the Delphi research via a survey	120
4.5.1	Composing the survey questionnaire	120
4.5.2	Survey participants	121
4.5.3	Survey questionnaire (web-based)	122
4.5.4	Survey participants and their industry	122
4.5.5	Analysis of survey data	126
4.6	Conclusions of this study into BIS management interventions	127

4.7	Contribution & recommendations	129
4.8	Limitations of this study	129
5.	EXPLORING GOVERNANCE PRACTICES	132
5.1	Introduction	133
5.2	Background of the research project	133
5.3	Research Method & Findings	134
5.3.1	Literature review	134
5.3.2	Expert panel	136
5.3.3	Research findings	137
5.3.4	Ranking the GSS data	141
5.3.5	Framework for BISG practices	142
5.4	Conclusions	143
6.	DESIGNING AND DEVELOPING THE ARTEFACT	146
6.1	Introduction	147
6.2	Explicating the problem to define requirements for the design	148
6.2.1	Explicating the problem per case	150
6.2.2	Five cases of DSR requirements for the design and development	150
6.3	Summary of explicating the problem and defining the requirements	194
6.4	Developing the SecuriMeter Artefact	197
6.4.2	The development of the SecuriMeter artefact on informational and data level	200
6.4.3	From initial functional design to prototyping	202
6.4.4	The structure and the technical specifications of the artefact	197
6.4.5	System layers in the artefact	204
6.4.6	Adhering to the guidelines for artefact design and development	211
6.4.7	Artefact development and maintenance	211
6.5	Conclusion to the Design and development of the artefact	213
7.	DEMONSTRATING AND EVALUATING THE ARTEFACT	214
7.1	Introduction	215
7.2	Demonstrating the artefact	216
7.2.1	Case 1: Demonstrating Key BIS management information in the MBIS artefact	217
7.2.2	Case 2: Demonstrating Key BIS governance practices and KSF questionnaire	222
7.2.3	Case 3: Demonstrating BIS maturity assessment questionnaire	226

7.2.4	Case 4: Demonstrating metrics in the MBIS artefact	228
7.2.5	Case 5: Demonstrating Stakeholder analysis in the MBIS artefact	236
7.3	Evaluating the artefact	238
7.3.1	Treatment validation	239
7.3.2	Evaluation objectives	239
7.3.3	Proof of concept to evaluate the artefact	240
7.3.4	Conclusions on the artefact evaluation	247
7.4	Discussion on demonstrating and evaluating the MBIS artefact	253
7.4.1	Evaluation of the knowledge items	254
7.4.2	Contribution to the artefact evaluation objectives	256
7.4.3	Comparison of the artefact	258
7.4.4	Comparison criteria	265
7.5	Additional insights after demonstrating, evaluating and comparing the artefact	277
7.6	Conclusions to the artefact demonstration and evaluation	282
8.	FINDINGS, CONCLUSIONS, LIMITATIONS AND CONTRIBUTIONS	286
8.1	Research findings	287
8.2	Research conclusions	296
8.2.1	Conclusions on the exploration into the conceptual framework for BIS (1).	296
8.2.2	Conclusions on the establishment of the DSR artefact (2)	300
8.2.3	Summary of the conclusions	301
8.3	Research risks and limitations	302
8.4	Research contributions and assumptions	306
8.5	Further development of the artefact	309
REFERENCES		314
ACKNOWLEDGEMENTS		333
INDEX		337
LIST OF ABBREVIATIONS USED		345
ABSTRACT		349
CURRICULUM VITAE		355
APPENDIX INDEX		356
Appendices that accompany Chapter 1		357

Appendices that accompany Chapter 2	352
Appendices that accompany Chapter 4	358
Appendices that accompany Chapter 5	360
Appendices that accompany Chapter 6	362
Appendices that accompany Chapter 7	364
Appendices that accompany Chapter 8	368
The Enterprise Engineering Network	370

For Nicole, Lolah, Mabel and "tante Lola"

FIGURES & TABLES

Figure 1	
The IS Governance Direct Control Cycle taken from Von Solms and Von Solms [57].	29
Figure 2	
The PDCA cycle on Direct Control Cycle of Van Solms & Von Solms based on Tewarie [66].	31
Figure 3	
Conceptual Model based on the Direct Control Cycle of Von Solms and Von Solms [71].	33
Figure 4	
Conceptual model with detailed BIS processes and data, based on Von Solms and Von Solms [71].	33
Figure 5	
Thesis structure including research questions based upon Johannesson and Perjons [73]	35
Figure 6	
Thesis structure with deliverables based upon Johannesson and Perjons [66]	37
Figure 7	
The structure of this thesis	40
Figure 8	
Qualitative and quantitative methodologies, taken from Recker [77].	45
Figure 9	
Frequency of applied information security research methods, from Lebek et al. [7].	47
Figure 10	
The paradigm and methodological choices in scientific research, based on Kyrö [99].	51
Figure 11	
Hevner's Design Science Research Framework [138].	63
Figure 12	
Overview of the framework for design science research [73].	67
Figure 13	
Multi-methods used in DSR, based on the Johannesson and Perjons framework [73].	68
Figure 14	
Proposed method and PDCA-based activities used to improve the maturity of BIS.	71
Figure 15	
Thesis structure, based on the DSR Framework of Johannesson and Perjons [73].	71
Figure 16	
Denoting the why, what and how, from Whetten [150], in relation to MBIS research.	73
Figure 17	
Enumeration of the theoretical constructs.	75
Figure 18	

Conceptual model of the BIS domain.	79
Figure 19	
Three lines of defence concept taken from the IIA report from 2013 [162].	81
Figure 20	
Greiner's growth model defines five stages of growth taken from Greiner [170].	83
Figure 21	
Business Information Security Management Meta Model.	85
Figure 22	
The PDCA cycle on Direct Control Cycle of Von Solms & Von Solms based on Tewarie [66].	87
Figure 23	
Information Security Governance according to Von Solms and R. Von Solms [210].	91
Figure 24	
The conceptual model of GDAC processes based on Starreveld et al. [211] & De Leeuw [213].	93
Figure 25	
Market segmentation based on number of systems.	101
Figure 26	
Conceptual model on mid-market interventions research.	103
Figure 27	
Evolution of COBIT.	105
Figure 28.	
Preselection of intervention candidates	113
Figure 29	
GSS expert meeting process flow	113
Figure 30	
Indication of the maturity level in 2010.	130
Figure 31	
Indication of the desired maturity level in 2012.	130
Figure 32	
Top 20 Practices for BISG according to the Literature and Experts Validation.	142
Figure 33	
Framework for BISG research	143
Figure 34	

Explicating the problem for the design of the artefact based on Johannesson and Perjons [73]	147
Figure 35	
Overview of the DSR framework based on Johannesson and Perjons [73].	149
Figure 36	
Sample of marking governance practices during the literature research.	165
Figure 37	
Research process, including research questions for defining BISG practices	167
Figure 38	
Conceptual model of the literature research, divided into relevant disciplines.	171
Figure 39	
Maturing Business Information Security assessment tree.	179
Figure 40	
Porter Five Forces model.	189
Figure 41	
Screenshot of the Qualtrics survey question about Porter.	189
Figure 42	
Research phase "developing the artefact" based on Johannesson and Perjons [73].	197
Figure 43	
Positioning of the artefact's based on Starreveld et al. [211] and De Leeuw [213].	199
Figure 44	
Design and development : the functional design of the MBIS artefact.	201
Figure 45	
Designing and developing the artefact: The technical design of the artefact infrastructure.	205
Figure 46	
Designing and developing the artefact: different layers in the artefact	207
Figure 47	
Deliverables from chapter 6 & 7 based upon the DSR framework of Johannesson and Perjons [73].	213
Figure 48	
Research phase "demonstrating and evaluating" based on Johannesson and Perjons [73].	215
Figure 49	
Case 1: Demonstrating dashboarding and policy.	218
Figure 50	
Case 1: Demonstrating dashboarding and policy.	218

Figure 51	
Case 1: Demonstrating dashboarding operational level of virtualisation vulnerabilities	219
Figure 52	
BIS processes and data based on Von Solms' Direct, Monitor and Control Cycle [57].	220
Figure 53	
Case 1: Demonstrating the policy setting and maintenance.	220
Figure 54	
Case 1: Demonstrating the evidence collection.	221
Figure 55	
Case 2: Demonstrating NPLF Likert score input via the management console.	223
Figure 56	
Case 2: Demonstrating the NPLF configuration via the management interface.	224
Figure 57	
Case 2: Demonstrating the BISG assessment in the artefact	225.
Figure 58	
Case 2: Demonstrating the six domains of the BISG maturity assessment in dashboard gauges	227.
Figure 59	
Case 4: Demonstrating the BIS organisation dashboard	229.
Figure 60	
Case 4: Demonstrating Business assessment (ISO) questionnaire	231.
Figure 61	
Case 4: Demonstrating evidencing-functionality	232.
Figure 62	
Case 4: Demonstrating BIS improvements and periodically changes via the IRO.	233
Figure 63	
Case 4: Demonstrating the metrics at the management level.	233
Figure 64	
Case 4: Demonstrating the metrics at the operational level (pen-test scores).	233
Figure 65	
Case 4: Demonstrating the NPLF scales which represent pen-test score.	235
Figure 66	
Case 4: Demonstrating evidence delivery for pen-test scores.	234
Figure 67	
Case 4: Demonstrating the dashboard information of the pen test score	235.

Figure 68	
Functional requirements for the stakeholder analysis	237
Figure 69	
Functional requirements for the Information Risk Overview	237
Figure 70	
Functional requirement setting for the asset inventory in the IRO	238
Figure 71	
Evaluation of the artefact: List of all the BIS assessments in the artefact	244
Figure 72	
Artefact alterations after the evaluation; a predefined set of interventions.	217
Figure 73	
Changes after the evaluation, warning screen for locking and unlocking assessment results.	250
Figure 74	
Artefact alterations after the evaluation: Document management system	251
Figure 75	
Evaluating the artefact; enforcement of treatment of risks.	251
Figure 76	
Evaluation: Artefact alteration after evaluations on IRO indicators.	252
Figure 77	
Design Science Research framework for transferring knowledge through the DSR artefact.	255
Figure 78	
Michael Porter five forces model.	255
Figure 79	
Michael Porter Five Forces model according to the research data from Case 5 .	257
Figure 80	
Artefact demonstration and comparison study research approach	263
Figure 81	
SecuriMeter Video demonstration on YouTube used for the comparison study	268
Figure 82	
ISF Video demonstration on YouTube used for the comparison study	269
Figure 83	
Methods to demonstrate and evaluate the artefact based on Johannesson and Perjons [73].	285
Figure 84	
The MBIS method and PDCA-based activities.	293

Figure 85	
Direct Monitor and Control Cycle including reflection internally and externally	297
Figure 86	
Spider diagram on the current status based on ISO27K (n=27).	299
Figure 87	
The spin-off process according to Nlemvo.	309
Figure 88	
The artefact maturing process based on Nolan Maturity Model of Organisations	311
Table 1	
Research methods and their contribution to BIS research.	69
Table 2	
Market segmentation according to the EU Commission based on headcount and financial figures.	100
Table 3	
Expert panel characteristics.	114
Table 4	
Top interventions according to experts.	119
Table 5	
Mid-market sectors and current versus desired maturity state.	124
Table 6	
Top intervention suggestions according to mid-market organisations.	126
Table 7	
Barriers according to companies in the mid-market.	128
Table 8	
Experts panel characteristics used in the BISG research.	136
Table 9	
Top 10 Business Information Security Governance practices in detail.	145
Table 10	
Case 1: Designing and developing the artefact. Key management information.	158
Table 11	
Designing and developing the artefact: Top 10 BISG and Critical Success Factors in detail	173
Table 12	
Designing and developing example 2 of the artefact: Top 20 BISG and Critical Success Factors.	175

Table 13	
Summary of five examples and their relationship with the five requirements.	195
Table 14	
Extract from the SecuriMeter issue log.	212
Table 15	
Summary of the 5 requirements in the artefact.	213
Table 16	
Planning of the evaluation of the artefact via a POC.	240
Table 17	
Summary of other operational-oriented security assessments in the artefact.	243
Table 18	
List of participant characteristics of the online survey test step 1a.	259
Table 19	
Participant characteristics in the comparison study step 1 b.	260
Table 20	
List of participant's characteristics of the GSS expert panel held on 10th August 2017 (step 3).	262
Table 21	
Type of test during the comparison including dates.	264
Table 22	
Final list of comparison criteria derived by the expert panel on 6 July 2017.	266
Table 23	
Expert scores on SecuriMeter matching the criteria ranked on rating.	270
Table 24	
Expert panel scores on ISF Accelerator matching the criteria ranked on rating.	273
Table 25	
Abstract of the 98 requirement suggested by the experts on multiple levels.	279
Table 26	
List of artefact requirements that are present in the SecuriMeter.	282
Table 27	
Summary of the evaluation methods used.	284

INSPIRATION

I am the manifestation of study, NOT the manifestation of money. Therefore, I advance through thought, NOT what's manufactured and bought.

-Kris Parker 1965

In 2008 I was motivated by a teacher who inspired me to do research and set up my own company. Like any other student, I liked teachers who inspire you, regardless of how old you are. This teacher captivated his classes by talking about his own personal experiences as a researcher and as an entrepreneur. What struck me most was the applicability of his research for contemporary organisations wrestling with the implementation of IT systems.

During my study we had long discussions on the necessity of doing academic research that actually makes a contribution to society. In my professional career as an entrepreneur – seeking better solutions that can contribute to delivering true value to organisations – I encountered managers and directors struggling with the implementation of Information Security. Encouraged by this teacher, I started my research journey in 2008, finding methods and practices that could help my company grow as well as help my customers improve.

In 2010 this same teacher assisted me in finishing my Master's degree in Informatics and another striking thing happened: the birth of my first daughter Lolah. These two life-changing events inspired me to approach this teacher to discuss a PhD. After some demotivating remarks about the long journey, the endless debates with promotor and students, and the worries that keep you up at night, he noticed that I was serious. So he invited me for a high tea in Delft, where we met together with our wives. I soon noticed that such journeys are not taken alone. I had the blessing of meeting my wife Nicole when I was only 21. As she is my best friend, she is also my life promotor and she motivates me in everything I do. Including this PhD.

So there we were, having high tea in Delft discussing not the topic, research questions and potential outcomes, but purely the intrinsic drives: what gives you energy and what takes it away. Or, as ice skating champion Johan Olaf Koss put it, "constructors". These are the people who inspire and have the ability to empower others. Now, at the end of my journey, I can tell you that these people are the most important source of inspiration and motivation if you decide to do a PhD. In 2013 my second daughter Mabel was born. During the year 2014 she gave me the strength to keep on going even when things might have set me back. I have had the pleasure of surrounding myself with such inspiring people who gave me the confidence and motivation I needed to complete my PhD. Due to them I never had moments of doubt or serious distractions along the road that could endanger my personal journey. There was always this teacher and my Nicole. After the high tea we decided that the teacher should become my mentor and co-promotor.

After completing my research work in 2015, another phase of my research arrived. I needed to finalise writing my dissertation. I founded great tips in a book “*Writing Your Dissertation in Fifteen Minutes a Day: A Guide to Starting, Revising, and Finishing Your Doctoral Thesis*” by Joan Bolker and in the project management approach that my promotor (the teacher) suggested to me. Another important constructor in that phase was Aart van der Vlist, at that time the CIO of UWV, who asked me to become the CISO of UWV and encouraged me to finalise my PhD alongside this demanding role. I had the pleasure of debating with him and he gave me the opportunity to put my academic work into practice. During that period again my teacher as well as my wife each played a vital role. That gave me the direction and energy that was necessary to continue and finalise my writing.

During the entire research I worked with organisations where I received all kinds of advice, especially the importance of touching base with practice and talking with people in all kinds of disciplines. From chairs of listed companies to security engineers. From students and teachers to regulators and government bodies. The entire list of all the people who gave me practically-oriented motivation are acknowledged at the end of this thesis. In particular, I would like to acknowledge my promotores Erik Proper and Steven De Haes.

Besides these acknowledgements I would like to pay my sincere respect to two people who were crucial to my PhD. First “the teacher” – who became my co-promotor, and later on my friend and mentor Hans Mulder. Hans and I established a sincere friendship based on deep respect and understanding. According to Kris Parker “*Real men are real friends, showing their real commitment*”. Hans revealed a great commitment to helping me finish my PhD. And my wife Nicole, who stands behind every adventure I undertake. Her friendship and love encourage me to do the right things at work as well as when being a father raising our two daughters. I think everybody needs a role model or friend: someone who shows faith in anything you do and has endless commitment. In my opinion teachers play a vital role in anyone’s life, whatever your age or professional status. I’m thankful to be able to lead, learn and teach. And surround myself with great friends.

Driebergen-Rijssenburg, 2018

1

INTRODUCTION

In this chapter I discuss the main motivations for this research project: on the one hand from my point of view as a practitioner and on the other hand as an academic exploration. This first chapter is my point of departure for a long research journey into examining ways to improve business information security maturity within mid-market organisations. In Chapter 2, I describe the numerous methods used in the following chapters, both to examine the topic as well as clarify the design and engineering of my artefact, which was created to improve the Maturity of Business Information Security (MBIS).

1.1. MOTIVATION BASED ON PERSONAL OBSERVATIONS

Organising Information Security (IS) within companies is complex [1]: When I started my consulting practice, security managers had a difficult job and that is still the case today. I observe companies struggling in their departmental silos with Excel and Word documents scattered throughout the organisation, with no integral view or one single source of truth that could be used to gain control. This becomes even more challenging as compliance and "control statements" represent a licence to operate for many firms. My main observation when starting my research in 2010 was that there was a lack of adequate knowledge and insights into relevant practices and parameters that could be used to improve Business Information Security (BIS) maturity. Insight in these parameters is necessary and, in some cases, compulsory due to various regulations [2]. Standardised frameworks such as the ISO27000 are being applied in order to implement Information Security. According to Siponen [3] "*these frameworks are generic or universal in scope and thus do not pay enough attention to the differences between organisations and their information security requirements*".

In practice I have seen the application of frameworks falter because they tend to become a goal on their own rather than a supporting frame of reference to start dialogues with key stakeholders. The absence of collaboration and exchange of perspectives that is based upon underlying data, is limiting organisations in their effective execution of IS. Kluge et al. [4] for example also noted that the use of frameworks as a goal on its own does not support the intrinsic willingness and commitment to improve information security maturity. This motivated me to examine the academic literature as well as "best practices" and the potential "barriers" that companies – and their key stakeholders - face when applying BIS. This is especially the case for mid-market organisations since they lack dedicated staff or sufficient budgets. During my quest I came across an inspiring research effort by Puhakainen and Siponen [5] that criticises information security approaches as lacking not only theoretically grounded methods, but also empirical evidence of their effectiveness. Many other researchers [6], [7], [8] have also pointed out the necessity of empirical research into practical interventions and preconditions in order to support organisations with MBIS. These theoretical voids, as well as the practical observation of failing compliant-oriented approaches, widen the knowledge gap [9]. This "knowing doing gap" [10] is what also motivated me as a business problem-solving researcher to examine the key concepts of this

phenomenon through Design Science Research (DSR) and, with this study, to build a design artefact that contributes to solving real problems.

1.2. MOTIVATION BASED ON LITERATURE

The widely used term Information Technology (IT) Security focuses mainly on information technology controls that are used to detect or mitigate information security risks. Recent research has shown that the number of IT security incidents has increased in recent years, as has the financial impact per data breach [11]. In 2009, an average of 25 percent of EU organisations experienced a data breach. The main factors influencing the increase in security incidents are the multiplication of data (Big Data), the increase in the number of high-speed internet connections, disruptive technology [12], [13] the Internet of Things, [14] (IoT), the increase in social media interactions [15], and the increase in cybercrime activities [16], [17]. Mastering this complex subject requires a team. Since IT security professionals must protect critical information, they need to know about the value of information and therefore the impact it might have if this information is threatened [18]. The IT risk management discipline requires capabilities, knowledge and expertise [19] that are clearly different from those that IT security professionals needed in the past. Hubbard [20] refers to the failure factor of insufficient 'expert knowledge' within impact estimations. He refers to the necessity of experience, beyond the fields of risk and IT security. This is why IT security increasingly also encompasses Human Resource Management (HRM) aspects [21], financial aspects [22], marketing aspects, etc. [23]. According to Von Solms, IT security goes beyond the IT department into business domains such as HRM, marketing, legal etc [24].

When we study Information Security, we observe an expanding range of disciplines related to securing businesses and their critical assets [25]. Traditional Information Security controls such as the segregation of duties in critical business processes are no longer the domain of just IT systems [26]. According to Neubauer and Heurix [27] business processes are permanently exposed to a variety of threats, organizations and are forced to pay attention to security issues. They state "*Although the security of business activities is widely recognized as important, business processes and security aspects are often developed separately and without considering different objectives*". These processes are designed [28] and maintained by the business, in this case with multiple people judging a certain business process (e.g. Segregation of Duties (SoD) in handling insurance claims). Another example is awareness training of employees, which is no longer in the hands of security technicians but part of integral business management [29], e.g. corporate culture [21] or HRM onboarding [30]. Business also includes the context that business is operating in and relationships with stakeholders who rely on information assurance, such as business partners, clients, shareholders, unions, pension funds, social communities and regulators [31]. Internal and external stakeholders of organisations who, according to the press, appear to have suffered security incidents such as ASML [32], UWV [33], ING [34], Yahoo [35], Gemalto [36], SONY [37], Dutch Tax Department [38], Diginotar [39] and Target [40] often suffer indirectly from security incidents. Those who are responsible – and accountable – in these

organisations are boards of directors and executive managers. These board members struggle with responsibilities and liabilities in relation to information security and cyber risks [18]. This can have serious consequences since they are also legally liable [40], [41]. Incidents such as Target [40] show us that the security of organisations is no longer in the hands of technicians or security officers only, but increasingly also in the hands of the CIO and CEO, employees, and it is subject to external influences. Altegrity [42], Diginotar [43] and Impairment Resources [44] reveal the power of negative perceptions and social media in causing a snowball of accusations that can ultimately lead to a firm's bankruptcy [45]. The Diginotar official investigation reports a lack of information security and audit practices [43]. This detailed report based on a trial in court [39] reveals failures in the security of systems prior to the hack, but also a lack of procedures around password management and patch management. The report also revealed the fact that proper in-depth due diligence was not performed by the buyer Vasco and Vasco was also not proactively informed by the seller about the prior security findings of the third-party auditors (ITsec Security Services B.V.). The penalties as well as the bankruptcy of Diginotar made the company's owners aware of their obligations. It also made stakeholders aware that bankruptcy can be the result of inappropriate management. It shed a stronger light on the need for proper Information Security Management (ISM). Nowadays Information Security Management is a strategic issue for business leaders and several institutions and communities have launched numerous initiatives to encourage business leaders to ensure good stewardship in this area [46]. The associated compliance obligations and the increase in security breaches have made many business leaders aware of its impact on the business continuity [47], civil and legal liabilities [43] reputation [48], [49], employability and financial position [50], [51] of companies. This is why Von Solms and Von Solms [52] have argued that Information Security Management (ISM) should be part of Information Security Governance (ISG) [52]. The IT Governance Institute (ITGI) states that ownership of data and its information risks are the responsibility of *businesses* and their owners [18]. Within the multidisciplinary context of Information Security we therefore use the term "*Business Information Security*" [53]. Managing Business Information is a prerequisite for improving Business Information Security maturity [54]. The International Federation of Accountants (IFAC) [55] and ISACA [56] describe information security as an integrated enterprise activity requiring proper governance of the work done in this area by the board and executive management.

In their 2006 publication on Information Security Governance (ISG), Basie and Rossouw von Solms [57] differentiate three levels: *The strategic level (Board of Directors and Executive Management)*, *the tactical level (Senior and middle management)* and *the operational level (lower management and administration)*. The figure below presents these layers and the associated activities. All directive-setting and controlling activities (including monitoring and evaluating) are seen as part of the strategic level of governance [57]. An example is the adoption of Information Security Control Frameworks such as the Information Security Forum (ISF) Standard of Good Practice. All activities designed to put these directives into practice take place at the tactical management level. The tactical level involves formulating

policies and guidelines, for example establishing minimum standards that the organisation needs to adhere to, such as incident management and supply chain management. The level below the tactical level is where these policies and guidelines are translated into procedures and working methods. For example, this is the level where monitoring software is configured which triggers incident response processes or imposes stricter guidelines for suppliers.

Governing the topic of Business Information Security is a relevant prerequisite for the Maturing Business Information Security process. Julia Allen of Carnegie Mellon University points out: "*Governing information security means viewing adequate security as a non-negotiable requirement of being in business. If an organisation's management and boards does not establish and reinforce the business need for effective information security, the organisation's desired state of security will not be articulated, achieve or sustained. To achieve sustainable information security maturity organisations must make information security the responsibility of leaders at a governance level, not of other organisational roles that lack the authority, accountability and resources to act and enforce compliance*" [54]. Increasing or maintaining the level of BIS maturity depends on the desired state an organisation wants to achieve. Determining the desired state of BIS maturity and the Governance of BIS is, according to Allen, a board-level activity. To arrive at a clearer definition of Business Information Security Governance we first consider the definition of Enterprise Governance as used by the International Federation of Accountants (IFAC) "*Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly*" [55].

This definition was modified by the international Information Systems Audit and Control Association (ISACA) as follows: "*Information Security Governance is the set of responsibilities and practices by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the organisation's resources are used responsibly*" [56].

Both bodies view information security as an integrated enterprise activity requiring proper governance.

Von Solms and Von Solms [57] mention in their research work that governance is relevant for Directing, Monitoring and Controlling, but also for evaluating, *reflecting and learning* from

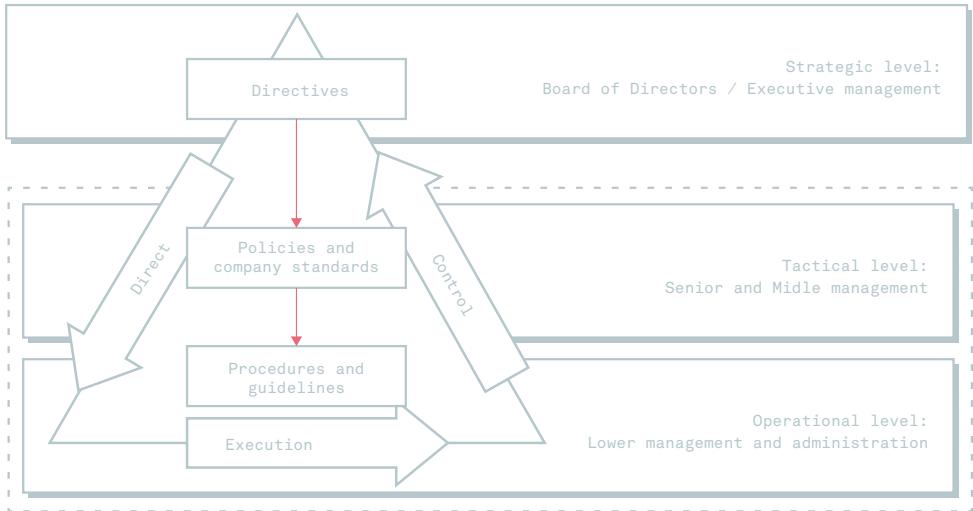


Figure 1: The IS Governance Direct Control Cycle taken from Von Solms and Von Solms [57].

incidents. Governance refers to "*all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organisation or territory and whether through laws, norms, power or language.*" [58] It relates to "*the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions.*" [59]. *Reflection and learning* from experiences as noted by Von Solms and Von Solms [57] is also mentioned by Lebek et al. [7] as a prerequisite for improving BIS [7].

PROBLEMS FOR THE MID-MARKET

Most of the contributions to the various best-practice publications by community bodies such as ISACA [56], National Institute of Standards and Technology (NIST), Information Security Forum (ISF) [19] and ITGI [18] are prescriptive in nature [60]. The objective is to guide organisations through a structured way of working, e.g. checklists, guidelines or sets of principles that can help companies achieve a desired state. Yet the problem for organisations lies in the fact that these prescriptive models and frameworks have limitations when they are implemented in the real world [3]. According to Siponen and Willison, these frameworks are perceived as complex and overwhelming [3]. They do not take into account all kinds of intangible factors such as stakeholder demands, culture [61], and industry type or company size [5]. According to studies by Siponen, [61], Kluge et al. [4] and Sanchez et al. [62], business leaders in mid-market organisations therefore find it difficult to understand where to start, and how to maintain certain business information security governance processes [63]. Kankanhalli et al. [63] investigated the effectiveness of IS and revealed the fact that mid-market organisations engage in fewer deterrent efforts compared to larger

organisations, even though these deterrent activities contribute to better IS. This is due to the amount of money needed to invest in IS and to a lack of sufficient knowledge [9]. The problem is that boards of directors in smaller organisations do not have an extended staff with advisers and also have other priorities, such as keeping 'the store' open and making money [63]. The problem with regard to mid-market organisations has the elements described below.

Due to an **increase in the use of technology** by society (Internet of Things) and the complexity of BIS, combined with an increase in **sophisticated cyber threats**, organisations have **limited insights** into potential risks and their impact on personal, financial and/or legal liabilities. Information Security tends to **stay at a tactical IT management level** (not at the strategic board level). **The absence of adequate knowledge and awareness** of insights needed to understand tactical and operational facts reduces the sense of urgency. In addition, organisations still practice **Information Security as an ad-hoc project** [64] in a fire-fighting mode, rather than as part of a continuous improvement cycle as proposed on Demings [65] PDCA cycle in most Information Security literature and adopted by Tewarie [66]. This ad-hoc approach leaves little time for reflection in order to improve and hinders the awareness of a continuous learning process and self-reflection [9], [67].

The main problem we aim to address in this research project is to contribute to the required knowledge sharing, build the necessary consensus on priorities (where to start), make informed decisions and create the necessary engagement among stakeholders. In this research we capture; knowledge sharing, consensus building, decision making and stakeholder engagement as the collective term "Collaboration".

We thereby encountered two challenges:

- Low stakeholder involvement and awareness
- The inherent complexity and dynamics of BIS due to more IT within organisations and society (IoT) and emerging –innovative- cybercrime methods.

Social interaction, collaboration and self-reflection are important precursors for determining what kind of tactical process data and operational log data needs to be captured for measuring, assessing and reporting to the strategic level so that managers and boards can form their opinion on BIS maturity performance. We want to examine if existing industry leading community practices such as International Organization for Standardization (ISO), SysAdmin, Audit, Network and Security (SANS), ISF, etc., can be considered as input for the required data analysis, measurement and reporting method.

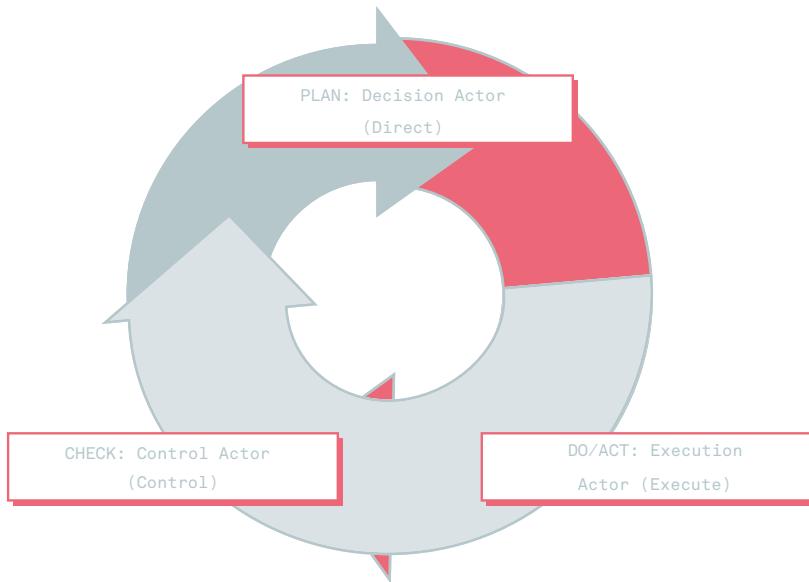


Figure 2: The PDCA cycle on Direct Control Cycle of Van Solms & Von Solms based on Tewarie [66].

1.3 PROBLEM STATEMENT

The *reflection and learning* noted by Von Solms and Von Solms [57] as well as Lebek et al. [7] is a prerequisite for continuously improving BIS on the people side [68], [7] as well on process [27] and technology. To include such a continuous reflective process within the existing models, each actor is required to develop feedback and feed-forward activities as part of the predefined processes. By doing this, a continuous *reflexive* process of *self*-learning and *self*-studying can result in continuous improvement [69]. A successful implementation of these self-reflexive processes is already adopted in software development via ‘retrospectives’ as part of daily team rituals, adopted from Lean process improvement [70]. To note this continuous reflection between the organisational layers and within the layers, arrows are added in the Direct Control Cycle in the figure below in order to address the problem we chose to work on. Since BIS is implemented within a dynamic environment, we also added this element in Figure 3. The conceptual model in Figure 3 represents the research area of this thesis and the scope of this research project is focused on the strategic level (Board of Directors).

This brings us to the problem statement of this research project: “*Organisations have to contend with BIS incidents. Board members struggle with their responsibilities and legal liability in relation to this topic, because it is not perceived and practised as a continuous collaborative discipline that is integrated into business management, with clear parameters and frequent contextual alignment*”.

'Parameters' here refers to a set of possible practices and interventions through which they can reach, monitor and maintain an integral view and achieve a particular level of BIS maturity.

BUSINESS INFORMATION SECURITY PROCESSES AND DATA

The key Information Security Governance layers of information risk and security to gain this integral view, based on Von Solms and Von Solms Direct Control Cycle [57], are highlighted in Figure 4. To better understand the BIS processes and data, on Governance, Management and Operational level, which are required for this integral view and do the BIS administration we describe each of them with some examples. The directive-setting objectives come from the strategic level. The risk appetite and accompanying policies are communicated to senior management in the form of requirements. Senior management is then mandated to put these policies into standards (e.g. technical, human and process requirements). These standards are applied in terms of all kind of risks (e.g. through maintenance of risk logs) and security (e.g. security action plans) processes and controls (e.g. general IT controls). These processes and controls rely on underlying processes such as service processes, change management processes and operational processes with clear requirements, such as firewall rule verifications, log handling, etc. Most of these processes are semi or fully automated. Some examples are Technical State Compliance Monitoring (TSCM), Vulnerability management (VM), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), Data Leakage Prevention (DLP), Threat Intelligence (TI), Secure Software Development (SSD) and Penetration Testing. All security requirements that are needed to keep risks within the risk appetite boundaries are stored in data repositories and documents such as Business Impact Analysis (BIA), Operational Security Guidelines (OSG), Security Requirement Lists (SRL), etc. (a detailed meta model is shown in Figure 21). Due to changes in legislation, technology and business environment these requirements frequently change. In most organisations documents reside on SharePoint servers, desktops and end-user computers (mobile devices) in spreadsheets [72]. This makes it an administrative burden to maintain a single location for such records and documentation management becomes a risk on its own since there is no single place of truth. This problem increases with the growth of the Internet of Things, changes in technology, software-based devices and emerging cyber threats. Regulated companies, such as financial institutions, are better in this respect, since managing information risk and security is part of their licence to operate and they tend to allocate sufficient resources for it such as dedicated security departments with dedicated Governance Risk and Compliance (GRC) tools [63]. Smaller, mid-market organisations struggle with this [62]. Within IT operations numerous security and service management processes are active in order to maintain a certain level of operational security control, given the information risks that may arise. All these processes provide input on the performance and compliance of information risk and security management. Prioritising and selecting the appropriate parameters that reflect the relevant operational data for the right audience is a

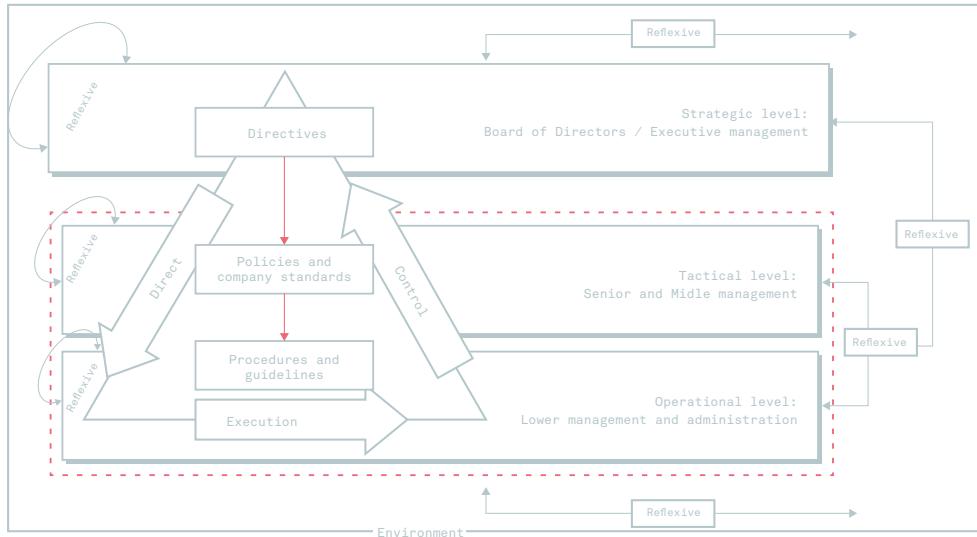


Figure 3: Conceptual Model based on the Direct Control Cycle of Von Solms and Von Solms [71].

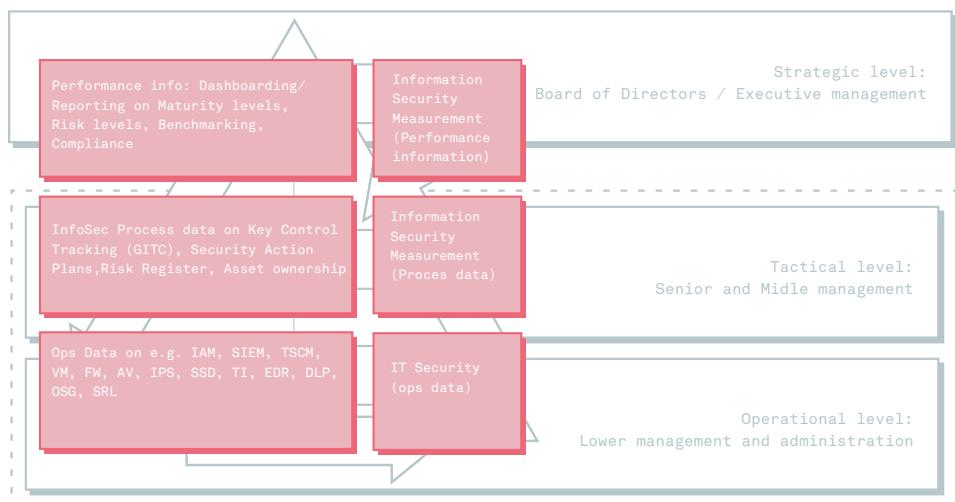


Figure 4: Conceptual model with detailed BIS processes and data, based on Von Solms and Von Solms [71].

cumbersome task. This requires collaboration between a number of stakeholders and target groups. Continuous measurement and reporting on the performance of risk and security processes is needed in order for boards and executive management to maintain control over BIS.

1.4 RESEARCH QUESTIONS, OBJECTIVES AND DELIVERABLES

Considering the issues mentioned above there is a need to; establish a more collaborative way of working among stakeholders when addressing the dynamics of the environment and the organisation, gain a more qualitative and integral view based on facts related to tactical and operational data, to secure an increase in awareness at board level, to employ a certain level of reflection and self-learning to achieve continuous improvement and to use accepted best-practice frameworks produced and maintained by existing security communities and bodies. Therefore, the aim of this research is to answer the following main research question "*How can we establish a method which utilises best practices and collaboration for improving BIS maturity?*"

In order to answer this main research question we follow Wieringa [73] to distinguish Knowledge Questions (KQ) and Design Questions (DQ). Knowledge questions provide us with insights and learnings that together with Design Questions contribute in the construction of the design artefact. This means that during the Design and development stages of this thesis (chapters 6 and 7) separate –requirement- design questions are formulated with the objective to design artefact requirements. The Design Science Research Framework of Johannesson and Perssons [73] is adopted and visualised in Figure 5 including the undermentioned research questions per step in the framework. Since mid-market organisations suffer from information risks and need to be helped with practical interventions at the managerial as well as at the governance level we distinguish the following questions.

To get an understanding of the underscoring key concepts of BIS we formulate this as the first research questions. This will be addressed in chapter 3.

1. *What is BIS maturity, based on the definitions derived from best practice and the literature? (KQ)*
2. *Which best-practice interventions are currently used to improve BIS maturity? (KQ)*
3. *Which barriers do organisations experience when applying BIS interventions? (KQ)*

Since BIS problems are more evident within mid-market organisations (they have limited budgets and IS staff, and are more likely to participate), this research focuses on mid-market organisations. The following additional questions therefore need to be answered:

4. Which barriers have been identified in mid-market organisations? (KQ)
5. Which of the identified BIS interventions are practical¹ in such organisations? (KQ)
6. What are the general organisational preconditions for the application of the core set of BIS interventions? (KQ)

These six knowledge research questions are answered via the explorative research described in Chapter 3.

An additional knowledge question is formulated to gain more insight into BISG practices and test the method.

7. What is a useful framework for Business Information Security Governance practices, according to the academic literature on the subject and the views of experts? (KQ)

This research question is answered via the qualitative research described in Chapter 4.

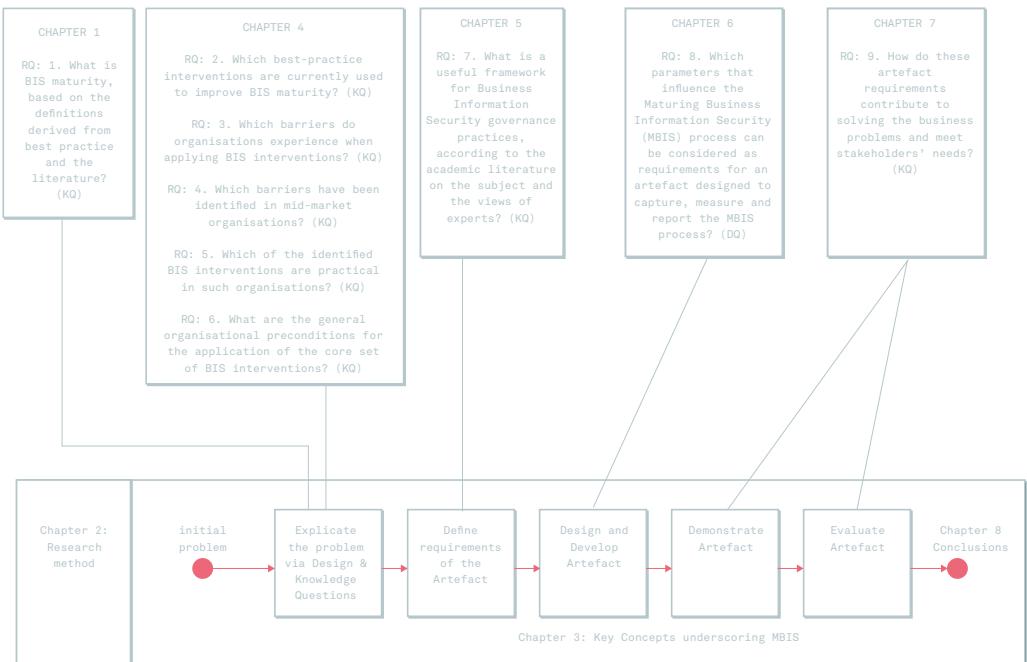


Figure 5: Thesis structure including research questions based upon Johannesson and Perjons [73]

1 In this research we define practical as 1) effective: the intervention or a combination of relevant interventions that effectively increase security and 2) easy to implement: to what extent is the intervention easy to understand and apply?

An additional design question is defined in order to determine which best practices can be used to measure, monitor and report on BIS maturity as well as further test the method to solve stakeholders' problems.

8. *Which parameters that influence the Maturing Business Information Security (MBIS) process can be considered as requirements for an artefact designed to capture, measure and report the MBIS process? (DQ)*
9. *How do these artefact requirements contribute to solving the business problems and meet stakeholders' needs? (KQ)*

The last two research questions are answered in Chapter 6 and 7 respectively.

Given the above research questions we have defined the following objectives:

- ♦ **Examining the key concepts and parameters that influence BIS maturity.** The collective term parameter is used to capture terms such as interventions, barriers, practices, critical success factors, knowledge items and working methods that are part of the MBIS process. I do this not intend to examine / scrutinise the current frameworks or models and the efficiency of these models.
 - ♦ **Designing and building an experimental artefact** with relevant parameters. To contribute to capturing the above-mentioned items by constructing an artefact which has the initial relevant requirements and the parameters of control needed to demonstrate that it contributes to solving MBIS-related problems. I refer in this thesis to an artefact experiment.
 - ♦ **Examining and defining a method** that addresses collaboration
- With these objectives in mind we aim to deliver the following deliverables as visualised in Figure 6:

RESEARCH DELIVERABLES

1 a) Parameters, insights and viewpoints that form a conceptual framework for BIS, and influences the BIS maturity at management as well as governance level (Board of Directors) as well as insights into factors that influence the BIS maturity.

1 b) A design artefact-tool that supports the administrative work (measuring and reporting), which can be used to report insights into the state of BIS maturity at multiple levels (strategic, tactical and operational) – using the parameters defined for reporting the BIS maturity of the organisation – to boards, owners and other stakeholders.

A defined analysis method which enables knowledge sharing, consensus building on priorities, informs decisions, enables stakeholder engagement, contributes to increasing of awareness and enables reflection.



Figure 6: Thesis structure with deliverables based upon Johannesson and Perjons [66]

1.5 THESIS STRUCTURE

This thesis is constructed to reflect both via theoretical and practical viewpoints in eight chapters. The structure of the thesis is shown in Figure 7. The purpose of this section is to provide a guide to give readers guidance on how this thesis is constructed and which chapter provide answers to the various research questions.

Chapter 2 provides a detailed description of the research philosophies and strategies that are relevant and applicable to Business Information Security research. It elaborates the strategies and methods that were chosen to answer the research questions and contributes to the rigour of the thesis. This chapter is based on two publications:

- Y. Bobbert, „Defining a research method for engineering a Business Information Security artefact,” in *Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum*, Antwerp, 2017. url; <http://ceur-ws.org/Vol-1838/>
- Y. Bobbert, „On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering,” *International Journal of IT/Business Alignment and Governance*, vol. 8, nr. 2, pp. 28-40, 2017. DOI: 10.4018/IJITBAG.2017070102

These papers focus on the several research methods used and it prescribes a Design Science Research approach for the development and implementation of an MBIS artefact.

Chapter 3 deals with key concepts underscoring the BIS topic. It presents a minimum set of concepts that are needed to answer the research questions. The outcome of this chapter answers research question one and forms the input for the conceptual framework for BIS that is applicable for the following chapters.

Chapter 4 provides the first step in the initial exploration of management practices that are effective and easy to implement by organisations in order to improve the Maturity of Business Information Security (MBIS). This research chapter is focussed on mid-market organisations and also involves them in answering some of the research questions. It includes preconditions, barriers and enablers of the maturing process that can be used in the following research phases. This chapter answers –knowledge- research questions one to six and proposes a Business Information Security conceptual framework for management interventions. An important finding in this chapter is the absence of Governance practices for BIS, this is addressed in the next chapter 5. Chapter 4 is largely based on the publication:

- Y. Bobbert and J. Mulder, "A Research Journey into Maturing the Business Information Security of Mid Market Organizations," *International Journal on IT/Business Alignment and Governance*, 1(4), 18-39, October-December 2010, United States, 2010. DOI: 10.4018/jitbag.2010100102

This publication describes the literature review, expert judgement via Group System Support (GSS) and mid-market validation of a core set of interventions that mid-market organisations can take into account for improving their BIS. The final core set of interventions are set as artefact requirement candidates in a later stage of the research.

Chapter 5 provides an extensive, in-depth literature survey of governance practices that are relevant for MBIS. It establishes a rigorous process of literature research and expert validation, leading to a core set of governance practices and critical success factors put forward in a framework that can be of relevance for Boards of Directors, which can be used in further research and design of an MBIS artefact. This chapter is based on the publication:

- Y. Bobbert and J. Mulder, "Group Support Systems Research in the Field of Business Information Security; a Practitioners View," in *46th Hawaii International Conference on System Science*, Hawaii USA, 2013. DOI 10.1109/HICSS.2013.244

This publication elaborates how the research among 4 experts was done to validate the literature on Governance practices via a collaborative process and documented in GSS. The title of this publication is: Group Support Systems Research in the Field of Business Information Security; a Practitioner's View. It was presented in Hawaii in 2013 and the outcome was taken into account to further establish and demonstrate the artefact.

Chapter 6 deals with the design and development of an MBIS artefact with a Design Science Research approach. There are five cases of artefact requirements that were adopted for building the artefact. All five cases have gone through the entire Design Science Research (DSR) cycle. This chapter was partly build upon two publications:

Y. Bobbert en J. Mulder, „Governance Practices and Critical Succes Factors suitable for Business Information Security,” in *International Conference on Computational Intelligence and Communication Networks*, India, 2015. DOI 10.1109/CICN.2015.216.

This paper describes the research process of collecting literature data on BISG and validates this via the GSS expert panel to establish a core set of BIS practices and Critical Success Factors. This research was conducted in 2011 and 2012. The derived BISG practices are used in the further establishment of the BIS artefact.

Y. Bobbert, „Porters' Elements for a Business Information Security Strategy,” *ISACA Journal*, vol. 1, nr. United States, pp. 1-4, 2015.

This publication reflects the research effort into strategic forces organisations cope with while drafting their strategic BIS plans. This chapter provides answers to design research question 8 and knowledge question 9.

Chapter 7 evaluates the way the artefact works, based on the five cases from chapter 6 and reveals its explicit contribution to solving practical problems that arise before, during and after the MBIS process. It also demonstrates how it solves problems experienced by stakeholders. It concludes with a thorough comparison study to demonstrate the relevance of the artefact functionalities and thereby further substantiate the answers to research question 8 and 9.

Chapter 8 contains the overall findings, conclusions and limitations of this research project. It reveals its practical and academic contribution and how the process of valorisation is realised through exploration and practical exploitation of the artefact.

The names of people who contributed this research project are blanked or scrambled for privacy reasons.

The appendices contain all the evidence data used to construct this thesis. These are separated data files that can be downloaded from the electronic archive: 10.17026/dans-zbu-hfdc.

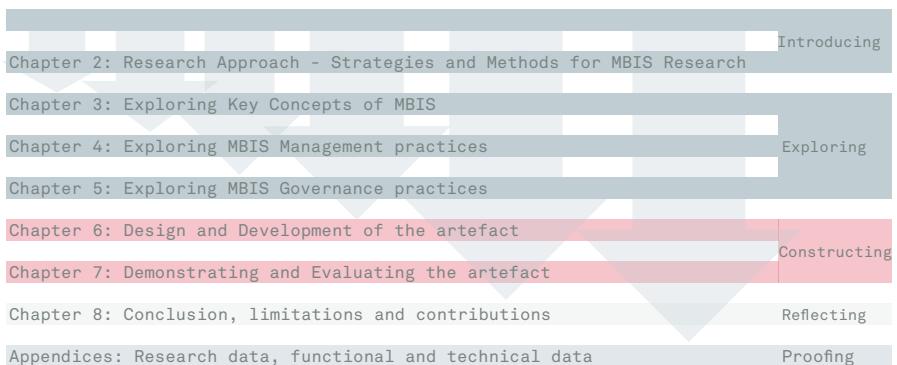


Figure 7: The structure of this thesis

2

RESEARCH APPROACH

This chapter deals with the research philosophies and strategies that are relevant and applicable to research on Business Information Security. It elaborates the strategies and methods that were chosen in order to answer the research questions and to contribute to the academic rigour of the thesis. This chapter consists of a survey of relevant research methods and techniques, followed by a discussion and research assumptions.

2.1 INTRODUCTION

In this chapter I explore a research methodology for studying the process of improving the Maturity of Business Information Security (MBIS) at the governance and executive management level. Within the domain of Business Information Security (BIS) there is little scientific research on research methodologies that has examined the parameters which influence achieving and maintaining an adequate level of Business Information Security Maturity. This chapter contributes to this discourse by examining several research philosophies and methods for conducting BIS research. It examines several philosophies, such as quantitative versus qualitative research and the differences in relation to BIS. It concludes by proposing a Design Science Research strategy which makes it possible to answer the main research question and it highlights the ontological and epistemological aspects within BIS and how they relate to the various qualitative methods. Ontology relates to how we view 'things' such as organisational change as a result of engaging in the information security maturing process. Epistemology relates to how and what knowledge is acquired and shared during that process. It deals with how we learn what we need to learn and how we can capture the right amount and depth of knowledge in the information security maturity change process.

This chapter is based on two publications that focus on the several research methods used and it prescribes a Design Science Research approach for the development and implementation of an MBIS artefact..

- Y. Bobbert, "*Defining a research method for engineering a Business Information Security artefact*," in *Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum, Antwerp, 2017.* url; <http://ceur-ws.org/Vol-1838/>
- Y. Bobbert, "*On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering*," in *International Journal of IT/Business Alignment and Governance, vol. 8, no. 2, pp. 28-40, 2017.* DOI: 10.4018/IJITBAG.2017070102

Governance, vol. 8, no. 2, pp. 28-40, 2017. DOI: 10.4018/IJITBAG.2017070102

2.2 SELECTING RESEARCH METHODS

2.2.1 QUANTITATIVE & QUALITATIVE RESEARCH

As explained in the previous chapter the BIS problem is too complex and ambiguous to be examined using a predefined method. Researchers describing methodological issues distinguish between qualitative and quantitative research methods. This classification "can be a helpful umbrella for a range of issues concerned with the practice of business research [74]." Quantitative research employs variables and measurements, whereas qualitative research does not. According to some researchers the differences go much deeper than the superficial issue of the application of quantification [75]. According to some writers quantitative and qualitative research also differs with respect to epistemological foundations [76]. Within quantitative research the principal approach is deductive in nature i.e. testing a theory with the help of quantitative data collection methods. Within qualitative research the principal orientation is inductive in nature. The objective is to generate theories. Within quantitative research the ontological orientation is objective. It has the view of social reality as an external objective reality, referred to as objectivism [76]. Objectivism is an ontological position that claims that social entities (e.g. organisations) exist in a reality that is external to, and independent of, social actors. Within qualitative research the ontological orientation is that of constructing the situation based on the details, and attempting to understand the reality behind it. This is often associated with the term constructionism or social constructionism [76]. "*Constructionism follows from the epistemological orientation of the interpretivist position to explore the subjective meanings motivating the actions of social actors in order for the researcher to be able to understand these actions*" [76]. Interpretivism is the epistemology that sees the role of the researcher as part of a 'social subject.' The researcher observes, analyses and interprets phenomena which he or she is part of. Positivists believe in applying methods from the natural sciences to study social reality. The epistemological orientation behind quantitative research is a particular form of positivism and it involves applying quantitative methods from natural sciences models to research the subject at hand. It would be wrong to suggest that several research methods cannot be combined. On the contrary, most of the research done in Information System Science or in Information Security involves a combination of qualitative and quantitative methods. Qualitative characteristics such as *explorability* or *complexity* can be combined with 'strong' quantitative characteristics, such as *generalizability* and *deductibility* [77]. Figure 8 visualises the various qualitative and quantitative methodologies.

Lebek et al. [7] reveal that most academic research (including 55% percent of IS research papers) is empirical and based on quantitative methods (see Figure 8). Non-academic based research projects and publications also largely depend on quantitative data sets. One of the best known practical-oriented research institutes, Ponemon, uses large quantitative data sets to derive qualitative statements [78]. Gartner and IDC also use numerous methods to gather quantitative data to generate qualitative theoretical assumptions. To a certain extent these institutes indicate the limitations of their research outcomes and the conclusions that

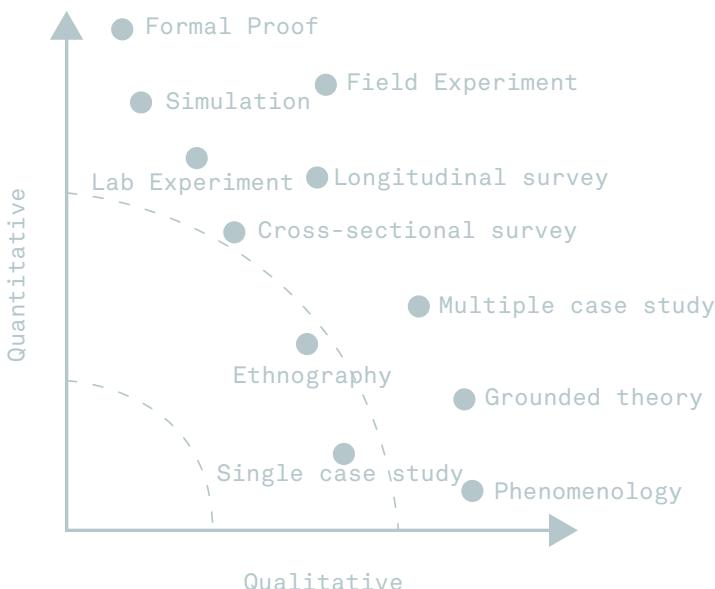


Figure 8: Qualitative and quantitative methodologies, taken from Recker [77].

they draw. For example, Ponemon raises an important limitation in the sense that they "decided to omit other important variables from analyses such as leading trends and organisational characteristics." Many of the ontological and epistemological issues within the information security area arise precisely from these *organisational characteristics*. For example, culture, attitudes, perceptions, etc. (relational mechanisms) are hard to capture without making use of qualitative methods (e.g. interviews, case studies and expert panel research). A paper by Lebek et al. reveals that scientific researchers still tend to focus on quantitative research methods when examining non-quantitative topics, such as awareness and behaviour. Figure 9 is the result of an extensive literature study that Lebek et al. performed from 2000 to 2012 on 144 publications dealing with employees' security awareness and behaviour. The researchers encourage the application of qualitative and interpretivist studies to explore more deeply factors such as user misbehaviour and a lack of user awareness. There is a need for more qualitative and interpretive studies in the BIS research field, as Workman et al. also found [6]. This is also acknowledged by Dhillon, who stated: "*There has been little research in information systems security that can be termed as interpretivist in nature. Generally functionalists do not even acknowledge the existence of such research efforts (ibid.). For them such approaches are 'abstract' and 'too general'"*" [79]. However, because of increasing dissatisfaction with the prevalent security approaches, there is a growing body of researchers who have begun to consider alternative philosophical viewpoints in their efforts to develop secure information systems.

Another relevant contribution was made by Abraham [80]. She did literature research on publications that examined intangible factors that influence user security behaviour, including the behaviour of senior management and decision-making skills [80]. Her study defined three major themes:

- Management and peer influences
- Deterrence efforts or sanctions
- Rewards and the level of employee participation in security efforts within the organisation.

Management and peer influence relates to the extent to which employees follow guidelines set by management (e.g. compliance regulations) through leading by “good example” or setting the “tone at the top.” If managers do not act in accordance with their own predefined guidelines, it is likely employees will follow that behaviour [81], causing IS programmes to fail. In her study Abraham noted a lack of studies that empirically evaluated the effects of management’s use of security practices on end users’ security behaviour.

Deterrence effects or sanctions relates to the effects these measures have on IS behaviour and IS adoption by employees. Rewarding employees can act as a motivator, creating commitment to IS. This was also found by Spurling in 1995 [82].

Rewards and the level of employee participation in security efforts in the organisation relate to the degree of positive influence user participation can have on IS strategy formulation and implementation. If users are involved at an early stage of the IS planning process (i.e. maturing towards a desired state) [82], [83], indicate that user participation contributes to “*improving security control performance through greater awareness, greater alignment between IS security risk management and the business environment, and improved control development*” [84].

Abraham examined 52 studies, studying individuals’ IS behaviour. She refers to a lack of qualitative studies that examine group interaction and behaviour using qualitative methods; “*information security is a complex phenomenon and its repercussions extend beyond individuals to groups and teams in organisations. While numerous studies have addressed end-user security behaviour, we lack studies that examine security group behaviour. Individuals can act differently in group environments [85] especially when groups are responsible for ensuring security. We identify the need for studies that examine the dynamics of security behaviour in group and team settings in organisations.*” This confirms the importance of qualitative research in this domain.

Three major studies over the last 15 years by Abraham [80], Lebek et al. [7] and Siponen [86] have examined the literature on intangible factors of MBIS success such as user awareness, management commitment, peer influences and behaviour. According to Workman, the limited amount of research in this area is restricting the IS field. Zooming

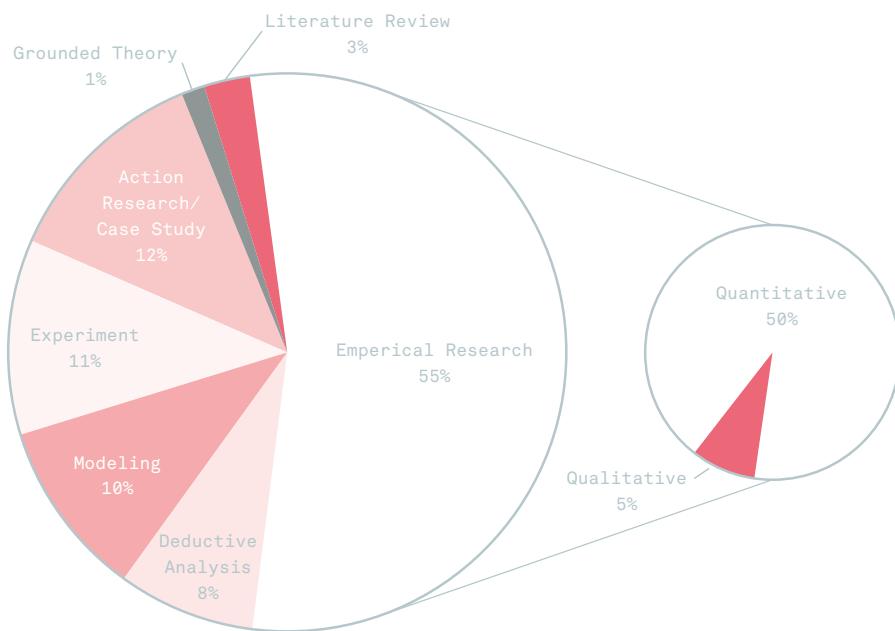


Figure 9: Frequency of applied information security research methods, from Lebek et al. [7].

deeper into a study by Lebek et al. [7], she states that only five of the 144 studies include >500 respondents. The authors argue that “*An empirical sample is relevant as long as it is representative and generalizable. Samples consisting of students and/or IS professionals do not reflect the population of interest. With reference to internal, external and construct validities, surveying students and IS professionals is seen more critically than having a smaller sample size, as long as it represents reality.*” Four publications; Siponen et al [87], Al-Omari et al [29], Pahnila et al. [88], Hovav and D’Arcy [89] interviewed >500 respondents, who were employees, i.e. valid representatives. The remaining studies involved professionals or students as respondents. This clearly indicated the importance of qualitative research on relevant stakeholder groups in order to formulate qualitative statements.

2.2.2 ONTOLOGICAL ASPECTS OF RESEARCH

The philosophy of ontology is about the nature of reality. Ontology raises questions about the assumptions researchers have about the way the world works and the commitment to hold particular views [76]. From a research perspective it raises the main question: *What is out there to know?* And how do we conduct our research to capture what we need to know. As Jan Dietz stated in his book Enterprise Ontology “*Ontology requires us to make a strict distinction between the observing subject and the observed object.*” [90]. Dietz continues: “*This also puts the researcher into another obligation that of clarifying the philosophical stance taken*

with respect to this subject-object dichotomy." The philosophy of epistemology examines what constitutes acceptable knowledge criteria in the field of study, knowledge perspectives such as adoption, capturing, transformation and presentation. Epistemology deals with the question: "How will we know what we need to know? It also deals with the subject-object dichotomy of the researchers' position. The position of the researcher can be viewed from an objectivist, subjectivist or constructivist standpoint. "*Somewhere between the objectivist and the subjectivist is the constructivist. Constructivists agree with the subjectivist that there is no absolute objective reality but a form of semi-objectivity reality that they call intersubjective reality.*" [90] This reality is created through the process of detailing the factors of influence (scope and context) and also the factors working behind them – intangible factors such as leadership or culture. In this research project we take the constructivist position, believing there is no absolute reality. Therefore the ontological 'reality' of the object is built through a continuous process of observing, analysing, negotiating and achieving social consensus among subjects.

So it's necessary to examine and explicate the ontological aspects in order to get a better understanding of phenomena. In this case the context (e.g. technology or business opportunities) influences the organisation as well as the 'construct' of the organisation (a certain view of the organisation). The scope and the context of the organisation determine why an organisation requires a certain level of BIS maturity, i.e. due to regulations, stakeholder demands [91] or the need for compliance with reporting guidelines [92]. The purpose of the organisation also determines the business objectives and therefore the Information Function (IF) of the organisation. This results in a certain need to protect critical information assets. The scope of the construct therefore also determines the scope of the object. So everything that is out there to know about the organisation and its characteristics needs to be examined in order to determine the level of knowledge required in order to understand "*what is out there to know?*"

As mentioned earlier in this chapter, much of the successful adoption of BIS phenomena is grounded in intangible factors [93], [87]. Studying tangible methods leading to successful information security (such as ISO27001, ITIL and COBIT) is common [94], [3], but studying intangible factors (e.g. knowledge and culture) alongside tangible factors and making both explicit is not.

2.2.3 EPISTEMOLOGICAL ASPECTS OF RESEARCH

Epistemology deals with the science of knowledge. It explores aspects of knowledge management and deals with research questions such as what level of knowledge is relevant to understanding and forming opinions on a certain subject [76]. To get a better understanding of "*knowing what we need to know*" at boardroom level, we highlight the important epistemological aspects of BIS.

"Knowledge has been described by Davenport and Prusak as a mixture of experience, values, contextual information, and expert insight that supports an individual to evaluate and incorporate new experience and information. An individual that is able to efficiently handle both new experience and information, and apply it in different scenarios, is often described as a "knowledgeable individual." Human knowledge, data and information altogether defines organisational knowledge, and when properly shared among organisational members, is a valuable asset which can be used to aid decision-making, improve efficiency, reduce training cost, and reduce risks due to uncertainty [9].

2.2.4 TACIT KNOWLEDGE

One concept of knowledge is tacit knowledge; this is the knowledge which is implicit in the heads of people within the organisation. It is hard to capture on a systematic way and hard to transfer via speech or in writing. Nevertheless, this form of knowledge can be very valuable during periods of change, e.g. knowledge of certain business processes or procedures, or knowledge of certain beliefs or behaviours that are typical of an organisation. It is hard to observe and pinpoint them, but these aspects clearly influence the "way people do things." Action learning is an effective method that can be used to generate and capture tacit knowledge.

2.2.5 EXPLICIT KNOWLEDGE

Explicit knowledge is knowledge that can be articulated, coded, accessed and verbalised. It can also be transferred to others. Most forms of explicit knowledge can be stored in data stores. Included in this type of knowledge for example are methods (NIST², SANS), frameworks (COBIT³, ISO), and other prescribed forms of guidance. The opposite is implicit knowledge. Implicit knowledge refers to a lack of awareness of certain knowledge [95]. Another aspect of knowledge is the way we generate knowledge among individuals and transfer it to others. This is what we refer to as *knowledge sharing*. Effective knowledge sharing mechanisms can help individuals to effectively share both implicit and tacit knowledge [9]. Nonaka [96] refers to "*a continuous dialogue between implicit and tacit knowledge via patterns of interaction, socialisation, combination, internationalisation and externalisation*". In line with Nonaka's dynamic theory of knowledge creation between groups and individuals and vice versa [97], Cook and Brown suggest that organisational knowledge is created via balancing knowledge and knowing [98].

In this research project we aimed to examine aspects of the knowledge management process that are involved in generating, capturing, recording, codifying, selecting, presenting and transferring knowledge. And the aspects of knowledge management content, i.e. *what is it what we need to know* in order to master a problem. In 2015 Flores published "*Information*

2 National Institute of Standards and Technology, NIST is an agency of the U.S. Department of Commerce.

3 Control Objectives for Information and related Technology (Source: ISACA)

security knowledge sharing in organisations: Investigating the effect of behavioural information security governance and national culture” In it he states an important aspect of knowledge sharing within the Information Security domain: “*establishment of knowledge sharing is beneficial as the individual knowledge possessed by information security professionals is transformed into organisational knowledge and transferred to end users and other stakeholders.* Flores refers to organisational learning in order to “*prevent security-related information and tacit knowledge from being laid scattered throughout the organisation or preserved by information security personnel as their personal property.”*

In Figure 10 the research methodology proposed by Fayolle et al. [99] is visualised from an ontological and epistemological perspective. What is visualised is that the process from ontological and epistemological knowledge is captured, analysed and presented using numerous methods and thus forms the methodology of this research project (to gain a more qualitative view of boardroom parameters).

2.3 RELEVANT RESEARCH METHODS FOR BIS RESEARCH

To explore methods suitable for qualitative research on Business Information Security I address the most important qualitative interpretivist methods that consider ontological and epistemological aspects. We start with literature research as a way to position the problem and to ground it in academic rigour. Then I examine the Delphi research method to elicit qualitative views and standpoints from experts in order to explore whether Delphi can contribute to solving the epistemological problem. Group Support System (GSS) research is examined as a method for overcoming knowledge issues related to ‘groupthink’ and knowledge sharing. Finally case study research (CSR) is explored as a qualitative method for in-depth research.

2.3.1 LITERATURE RESEARCH

Examining the literature is an essential starting point for each research project. It helps researchers – by conducting a thorough analysis of the existing body of knowledge – to make a new contribution. Literature research helps the researcher, whether a scientist or a practitioner, to engage critically with the ideas and knowledge of other writers. Within literature research we define three types of knowledge: 1) knowledge about the domain and topic of interest. 2) knowledge about relevant theories, which helps frame research questions. 3) knowledge about relevant research methods in order to get answers to research questions and thus develop new knowledge, build innovative artefacts or articulate new questions [77]. When encountering a business problem, it is not always clear what to examine in order to arrive at answers and solutions that can explain and potentially solve the problem. Business problems are usually not well defined and lack clear boundaries.

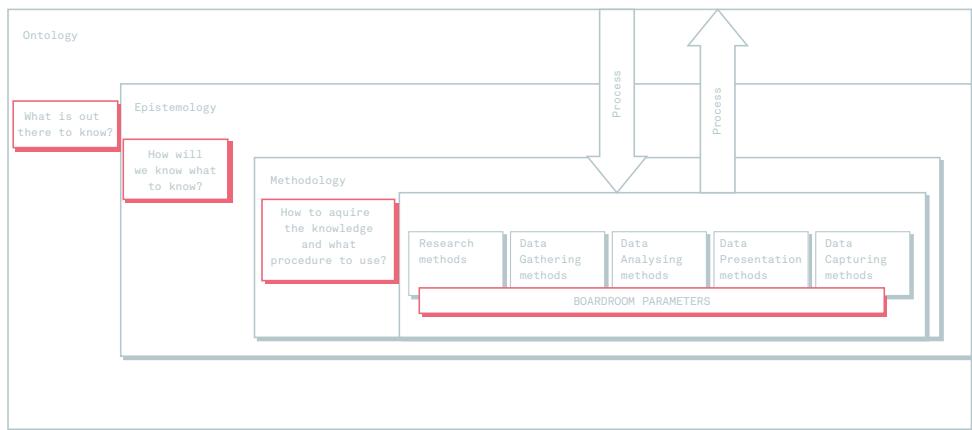


Figure 10: The paradigm and methodological choices in scientific research, based on Kyro [99].

Golden-Biddle and Lock [100] view literature review as an important starting point for storytelling. They distinguish two processes in the way the literature review is carried out and expressed. *Constructing intertextual coherence* refers to the way literature is analysed, structured, synthesised and presented in such a way that the researcher demonstrates his or her contributions to and relationship to the research reported. It thus appeals to readers' interest. The techniques for *constructing intertextual coherence* involve: synthesising coherence, progressive coherence and non-coherence (this refers to a lack of consensus among practitioners). In Information Security research papers we observe a lot of consensus among academia, but there is considerable disagreement among practitioners [9], [3] [84] on how to frame this embryonic topic and the numerous problems it causes. The disagreement among practitioners is also caused by the multiplicity and complexity of solutions or advice [9]. This suggests a need for more academic research to provide clear definitions and it also highlights the importance of more empirical research [6]. Explicating a problem with academic rigour involves thoroughly decomposing the theoretical concepts contributing to the problem and systematically deriving concepts and related topics from the literature. Conducting *systematic literature review* is described by Tranfield et al. The authors recommend systematic literature review to improve the quality of business management research, which they argue tends to '*lack thoroughness*' and reflects the bias of the researcher. [101]. The authors also propose this method for audit trailing of the researcher's steps and decisions during the research process. Research "that involves systematic literature review is argued to be more strongly evidence-based because it is concerned with seeking to understand the effect of a particular variable or intervention that have found in previous studies" [101].

In the case of Information Security numerous technology vendors produce research reports that lack a clear audit trail of the scope, methodologies used and timeline, as well as framing of the concepts and the validity of the respondents. Saunders et al. point out that some researchers become uncritical due to the influence of previous research. Often their work is little more than annotated bibliographies [102] – individual items that are selected because they fit what the researcher is proposing. The outcomes of, for example, vendor research reports are based on different methodologies and the outcomes are often tendentious. In some cases they leave it to the imagination of consumers or business decision makers to work out what methodologies were used. In the case of BIS research the entire community would gain more trust and credibility by adopting more systematic and evidence-based research strategies in their business propositions and practices. The sector tends to suffer from "Fear Uncertainty and Doubt (FUD)" [103] because of selling arguments, which causes a psychological side-effect: *cognitive dissonance* [104] within the information security practitioner community.

USING LITERATURE REVIEW FOR BIS RESEARCH

When examining executives' practices and establishing the level of governance based on the literature, it is advisable to code or rubric the literature based on certain criteria. The codes relate to criteria that the researcher can identify before, during or after the literature research as relevant to the research project. Coding literature also establishes a more organised and structured way of working. For BIS research we can identify for example two genres: academic literature and practitioner's literature. Another successful example of coding in the quest for BIS governance parameters based on the literature is presented by De Haes and Van Grembergen. The authors researched Business and IT Alignment and Governance practices. They distinguished governance practices based on *structure practices, process practices and relational mechanism practices* [105]. This distinction made it easier for business managers to implement the presented list of practices in their organisation. This same classification of structures, processes and relational mechanisms was later adopted by ISACA and integrated into the COBIT5 for Information Security guidelines [56]. Thanks to the rigour of the researchers and the ISACA Institute, these governance practices were embraced by the practitioner community.

There are no strict guidelines for conducting systematic literature research. Tranfield et al. [101] propose a so-called 'funnel', ranging from outlining the choice of certain words and databases used to narrowing down to a brief overview of key ideas and themes to compare and contrast the research of the key writers. The aim is to highlight key concepts and to detail relationships. This is necessary to define your own contribution in the form of fresh findings [76].

Literature research encourages academic and practice-oriented researchers to think critically about their subject and scrutinise their concepts, constructs and viewpoints in order to clearly explain the research problem and formulate their research questions. When it

comes to BIS, systematic literature reviews form an important basis for business advice. The main reasons for using *systematic literature review* principles in BIS research would be to move away from FUD towards rigorous thoroughness, and to remove researcher bias. Bias is a pitfall for interpretive researchers. Thus, literature research is proposed in BIS research as the basis for an objective, unbiased, structured point of departure. This is why I define two levels of literature research in this thesis. One is literature research used to substantiate the major concepts, as described in Chapter 1. This generic literature research is also applied in Chapters 4 and 5. The second is literature research used as a method for examining a specific problem encountered in the business environment. Literature research is therefore a research method that can be used to investigate a problem, articulate a problem statement and define requirements for an artefact designed to solve that problem. This is what is described in this chapter.

2.3.2 THE DELPHI RESEARCH METHOD

Delphi research is mainly used to gain a deeper qualitative view of a certain phenomenon – to examine propositions, theories and viewpoints through the use of an iterative process [106]. Delphi can be used to elicit views from experts, but also standpoints of user groups, expert groups, stakeholder groups and consumer panels. This form of research enables the researcher to propose practices or theories and, through a number of iterations, get a group of respondents to form a qualitative view [106]. The respondent group can then either rank, prioritise or scrutinise this view. In the case of Information Security it enables the researcher to position organisation-specific elements that might influence the process or the content. For example, a researcher may have derived certain best practices from the literature but want to validate them with a certain group of respondents. Schmidt et al. [107] developed a ranked list of common risk factors for software projects as a way to build theory about IS project risk management. The participants were three panels of experienced software project managers from Hong Kong, Finland and the United States. Thus, Delphi is not geographically limited. Delphi research can be performed via the internet in the form of survey questionnaires and it is thus possible to approach a large set of respondents throughout the world. Okoli et al. studied the difference between traditional surveys and the Delphi method [108]. One of their main findings was construct validity. "*In addition to what is required of a survey, the Delphi method can employ further construct validation by asking experts to validate the researcher's interpretation and categorisation of the variables. The fact that Delphi is not anonymous (to the researcher) permits this validation step, unlike many surveys.*" This enables the researcher to validate certain findings from the Delphi method at a later stage. In addition of traditional surveys, "*Delphi studies inherently provide richer data because of the numerous iterations and the response revision due to feedback. Moreover, Delphi participants tend to be open to follow-up interviews.*" [108]

A crucial factor in qualitative research is the personality of the respondent and the researcher. Potential bias is therefore a pitfall for all qualitative research (e.g. via interviews and case

study research), but it is limited within Delphi research, because of the distance between the researcher and the respondent as well as the anonymity of the participants. This enables an objective representation of the research process, with limited personal interference. Initially the knowledge of the researcher is used as input for the Delphi research method. The researcher can collect concepts, constructs or viewpoints about the topic from, for example, the literature. He or she collects a specific set of data about a topic (content) or about a certain approach (process) and it is then judged by the respondents. De Haes and Van Grembergen used the Delphi research method to study IT governance practices from numerous literature sources [109]. They used a pre-ordered dataset which was ranked by experts according to a predefined set of criteria. This gave the researchers not only new insights into the phenomena, but also a prioritisation for practical use based on "ease of implementation" and "easy of effectiveness", with the objective of establishing, in collaboration with experts, a set of core practices that practitioners can use in the field. The Delphi research in this case was used to generate knowledge about the content e.g. practices but also new knowledge about the process of applying the practices in a certain sequential order. This rigorously developed core set of practices has been successfully applied by numerous companies. Their research contribution shows that the Delphi method is a qualitative method that can be used to generate, gain, transfer, capture and report knowledge elements which can immediately be applied to solve business problems. De Haes and Van Grembergen also applied – as an extension to their earlier work – additional extreme case study research to benchmark their previous results [105].

Kim Maes did similar work in his PhD research project [110]. Maes collected elements affecting IT investments by making use of the Delphi method. He used the collective knowledge of a large number of experts to derive a set of practices that contribute to the value proposition of IT investments. So, he made use of experts to create new knowledge on a certain topic and transferred that knowledge through his publications and consulting work. With his research, Maes contributed to academic rigour while making a practical contribution.

APPLYING THE DELPHI RESEARCH METHOD WITHIN BIS

When seeking parameters for MBIS, via anonymous views from experts, the research by Maes, De Haes and Grembergen seems promising, in particular for generating standpoints, practices and criteria among experts and thus solving the epistemological problem of knowing too little or too much. In the case of research about Information Security strategy formulation, the decision-making process for those at this strategic level is evident [111]. In other words, we can derive and share knowledge about strategy but, as long as directors or executive managers do not take this knowledge into account, it is useless. So to effectively transfer the knowledge to other groups, in order to establish the learning organisation [9], we might consider the same or perhaps other qualitative methods, in order to transfer propositions to other groups (such as management teams, board of directors, project teams, etc.).

2.3.3 GROUP SUPPORT SYSTEM RESEARCH

The application of GSS for large-scale and longitudinal research has been identified by De Vreede et al [112]. De Vreede et al. substantiated their findings with the following case studies:

- Boeing Aircraft corporation (USA)
- 654 participants in 82 GSS sessions (average team size 7.9);
- International Business Machines (IBM) (USA)
- 441 participants in 55 GSS sessions (average team size 8.0);
- Nationale Nederlanden (Netherlands)
- 414 participants in 41 GSS sessions (average team size 10.0).

A case study from The Dutch Policy Academy was based on 45 GSS sessions from 2005 to 2011 in which 763 Academy students participated [113]. The average group size was 16.9. Research on GSS shows an average of 8 to 17 participants per session. The literature indicates in these cases that the number of items to be generated organised and evaluated ranges from 30 to a maximum of approximately 50 items [113]. The rationale behind the planning and guarding of a limited number of items – which is part of the preparation of the meeting and the responsibility of the facilitator is the 'limited' time and 'processing' power of teams with group sizes up to 17 participants. The current research project involved smaller groups such as security experts, Boards of Directors and Management Teams. The size of these teams is often two to four times smaller than the average group size.

Focus/expert groups make it possible to elicit views and perceptions from a diverse group of experts [114]. When making use of facilitating functions such as a computer-assisted analysis of qualitative data (CAQDAS), it is essential to respect the GSS ground rules as researched by Hengst in 2005. Her research presents an approach to gathering valid information for determining the optimum set of facilitation functions and ground rules that have been applied in a current research project [115].

- Generating new data between the participants and thus creating awareness and transferring knowledge
- Testing assumptions
- Sharing relevant information (knowledge) with the participants
- Using specific examples and agreeing on what important words mean
- Explaining reasoning and intent
- Focusing on professional opinions, not personal opinions
- Combining advocacy with inquiries
- Jointly designing next steps and ways to test disagreements
- Discussing 'undiscussable' issues (barriers)
- Ranking outcomes (parameters or intervention candidates)
- Comparing outcomes and discussing variables.

INFLUENCES OF GROUP SIZE IN GSS

There is no 'ideal size' for a focus group [116]. "*Focus group sessions can be structured, or unstructured, depending on the purpose of the research. The group discussion is led, and controlled, by a facilitator whose role it is to: stimulate a free-flowing discussion; help members share their experiences; elicit the views of all participants; keep group members on track; and capture responses.*" [114] The role of the facilitator is important in order to avoid the "Asch Effect" where certain individuals dominate the group and therefore the outcome of the discussion [117]. Since group size influences the ability of groups to achieve a productive outcome [118] the selection of the right (number of) experts is key to obtaining collective intelligence. The quality of the outcome of the group discussion ought to be better than individual opinions before the discussion [119]. Inviting the right number of participants with the appropriate kind of expertise is an important step. If their number is too high, there might be too much "noise." Too few participants may result in insufficient qualified data to generalise the opinions of the experts. Moreover, the number of items to be discussed is an important variable in the setup of the meeting. Participants discuss comprehensive lists of items and a number of measures are necessary to facilitate this process. One measure for retaining attention during the meeting is to introduce a 'carrousel' in which each expert starts with a different list of items to comment on. After this first round, the expert reviews the comments of the expert sitting next to him/her. In this way, all the other lists of items are reviewed. This measure also speeds up the process of generating unique comments. Once all the comments by individual group members have been generated, the group discusses them – guided by the facilitator. Another way to handle many items is to ask every participant to study the items on the agenda in advance. Invited experts are then also able to verify whether they really are experts in the domains that are to be discussed.

GSS FOR KNOWLEDGE SHARING

In "*How to make collaboration work*" Strauss [120] examines how to build consensus and to generalise opinions phase-by-phase with small groups. Designing systems to support collaborative processes for knowledge gathering, capturing and sharing and formulation of alternative viewpoints is grounded in areas such as group decision-making, nominal group techniques [121], the Delphi method [106], computer-mediated communication systems [74], social judgement theory and decision theory as well as online communities [122]. Apart from respecting the ground rules of working with GSS in qualitative research, recording is also relevant for reviewing the process of discussion, opinions, brainstorming and decision-making. And recording can be used to analyse the session afterwards. Another reason for recording the GSS sessions is to support claims about "reliability and truth" [75]. Using an audio-visual recording mechanism substantiates observations made by the researcher (makes them reliable) and gives readers the ability to form their own opinions about the perspectives of the participating experts. Pols [123] used GSS to overcome interpretation problems that normally occur when sending out questionnaires. Each individual interprets these differently and this reduces the reliability of blind surveys as a qualitative method. GSS was used to increase understanding of questions.

APPLYING GSS IN BUSINESS INFORMATION SECURITY RESEARCH

However, GSS is only rarely applied as a system in which hundreds of participants share their knowledge about hundreds of items in a specific domain [124]. Business Information Security research presents an opportunity for carrying out large-scale longitudinal research. Especially because nowadays knowledge is mainly gained at the micro (organisation) level and there is limited knowledge exchange between industries, countries and jurisdictions. So the knowledge stays in the company and sometimes within the department [9]. The opportunity for larger scale longitudinal research lies specifically in gaining knowledge at the organisational level and using that data, collected with GSS system technologies, to establish a collective knowledge base. This larger set of data can then form a frame of reference for a certain industry, country or community and thus contribute to other sectors, countries or communities. The application of GSS for such large-scale longitudinal research has been identified by De Vreede [112]. He and his co-authors substantiated their findings with hundreds of cases. Another author, Murray Turoff states that using data from large data sets gained from larger groups can be very helpful to generate more and better ideas. He also encourages users to establish process variables. This is desirable because "*when the group represents an organisational membership this is probably a very feasible and desirable pre-step to the execution of the examination of the issue*" In respect to BIS in boardrooms or management teams this means collectively sharing knowledge and gaining group consensus at the beginning of the problem as well as on the solution. Turoff continues: "*anything that will promote involvement in the design will increase motivation and the results of participation during the process*" [125] According to Pai [67], this early stakeholder engagement is also relevant for solving epistemological and ontological problems and it makes GSS suitable as a "collaborative research method".

Group discussions, thinking and decision-making have been evolving as web-based technologies, such as WebEx, Facetime, Google+, Skype, can facilitate this process [125]. Individual input can generate a large set of meta-data that represents a collective knowledge base. "*Over time this sort of system would become an evolving knowledge base for virtual or online communities*" [125], [126]. In 2012 Feledi and Fenz [1] investigated how machine-readable information security knowledge was shared between information security experts from different organisations on the basis of a web portal. According to Moorsel et al., knowledge-sharing facilities such as GSS provide the solution to the epistemological problems of knowledge capturing, sharing and thus feed decision-making [127]. GSS is therefore proposed as a qualitative research method for knowledge management and the decision-making process within the field of Business Information Security.

The field of BIS suffers from many problems. The first is a *sense of urgency* within the boardroom. The second is ad-hoc approaches to solving problems. Approaches can involve an attitude or a perception (how we think) or can be the approach to a certain problem, whether process-based or ad-hoc (how we do it). The approach to the topic is mainly formed

by knowledge of the domain (contextual knowledge) and in-depth knowledge. An absence of knowledge fails to trigger individuals' latent behaviour, beliefs and attitudes towards the problem and therefore the way an individual is trying to solve a problem, i.e. via an ad-hoc intervention or embedding it in the processes of the organisation. This gap between what we know but don't do is referred to as the knowing-doing gap [10]. This is a gap that often prevents organisations being successful in a certain practice. GSS can bridge this gap in two ways, first by making the problem explicit based on theoretical constructs and concepts. Second, by establishing awareness and a mutual level of knowledge among those involved with the problem (object and subject) to stimulate group dialogues and facilitate socialisation [96] thinking [7], discussions [129] and using the decision-making process for strategic planning [67].

2.3.4 CASE STUDY RESEARCH

Case Study Research (CSR) is one of the most popular ways of doing qualitative research [75]. It is widely used within Information System research, by business management to gain a qualitative view of a certain phenomenon. Robert Yin defines CSR as an empirical inquiry that is used to investigate contemporary phenomena within a real-life context [130]. It's especially useful when boundaries between the phenomena and the context are not clear. Case studies provide deeper qualitative insight into a phenomenon, making use of numerous data sources and numerous data collection methods, such as documentation, observation, interviews and secondary data gained from other sources. CSR is used for confirmatory purposes (testing theories) and for exploratory purposes (building theories) [131], [77]. Another objective of CSR is to explain. Typically interpretive CSR seeks to explore possible explanations.

Within CSR we distinguish two types of research: positive and interpretive. The positive researchers' ontological view of the world is objective – they act as external observers. They mainly collect, analyse and interpret data 'from a distance' to judge if it counts as evidence and knowledge. And they present the data with a rational view of the phenomena. Positive CSR involves formulating hypotheses and testing them with case study findings. Researchers explore the phenomena and generalise, primarily based on statistical data. Interpretive research involves focusing on research options to get a deeper understanding and interpretation – mainly to find explanations based on one's own interpretation and social view of the world (as part of the research subject). When conducting case study research it is essential to understand the researcher's own position towards the subject and the object to be researched, both from an ontological and an epistemology perspective.

There are two ways to conduct CSR: either via a single case study or through a multiple case study. A single case study provides an opportunity to explore a certain phenomenon within a certain organisation but it is limited in terms of the generalisability of the data. Multiple case study research provides us with more data to be analysed, replicated or compared and

therefore makes it easier to generalise findings. Generalisability of findings is desirable in Business Information Security research. First of all because the data collected from cases, for example successful practices can be replicated elsewhere (knowledge gained from the first case is transferred to others). Secondly, a deeper qualitative analysis of the data might provide more in-depth knowledge in certain industry practices. Through conducting numerous cases, and capturing this knowledge, cross-sectional knowledge sharing can take place.

CSR can involve numerous methods: interviews, observations, surveys, etc. and the data can be captured via recordings, transcripts, video, questionnaires, documents, reports, field notes, diaries, etc. Gathering this type of data within cases is limited because most of the time it is not recorded in the body of knowledge. The researcher must be alert to the fact that data is usually uncertain, complex, incomplete and messy. This can be mastered by thorough preparation. For example, by analysing the pre-collected information about the object and subject, preliminary discussion and during the CSR recording all the data. This leads to a better reading of the data afterwards to derive main issues and focal points, which can be interpreted from theoretical perspectives (*bringing in the theory*) and by reflecting on the data (*questioning the theory*).

Gioia et al. [132] proposed a data structure model for CSR. The authors defined the steps for gaining first-order concepts and deriving second-order themes. This eventually leads to aggregated dimensions that characterise the main problem. The authors have tried to articulate an approach that enables both the creative imagination and provides systematic rigour in conducting qualitative research. The Eisenhardt [131] approach is an example of constructing evidence collection in such a way that the data is collected, recorded, analysed and reported in a very precise and structured manner. "*The theory is emergent in that it is developed by recognising the patterns of relationships among constructs within and across the cases.*" In her paper "*Building Theories from case study research a process that utilises case study research* [131]" Eisenhardt presents a claim that a "*triangulation of methods (interviews, observations and archival sources) provides stronger substantiation of constructs and hypotheses.*" Moreover, the combination of data types can be highly synergistic. "*The qualitative data are useful for understanding the rationale or theory underlying relationship revealed in the quantitative data*" [131]. So, in situations where it is desired to combine quantitative data with qualitative data and understand the rationale behind it, case study research – with a structured process of data collection, recording and reporting – is preferred. To increase reliability and objectivity, Eisenhardt advocated working in research teams, using multiple researchers with clearly predefined assigned tasks. This creates more confidence in the findings and increases the likelihood of surprising findings [131]. It also permits knowledge sharing among researchers and transferring lessons learned to the business setting.

Constructing arguments based on CSR traditionally relies on the traditional criteria of "Reliability, Validity and generalisability" [74]. New insights into these criteria are added, such as objectivity and accountability (*who is accountable for the objectivity?*). Another new insight criteria introduced by accounting scholars is 'auditability' (*show how it is done*) [133] and 'transferability'. This refers to the fact it can be used elsewhere and it is action oriented.

In BIS research the findings are sometimes biased by the researcher's or the interviewee's personal motivations. Sometimes information is held back or is simply unknown (i.e. *blind spots*) [134], [130]. This requires additional skills from the researcher, such as questioning skills [135]. It can also be resolved by working in teams (of two to three persons). Another limitation is the fact that interviewing requires attention by the researcher in asking questions, observing non-verbal communication and listening, all at the same time. This multi-dimensional perspective can also be covered by working in pairs [131]. In some areas (e.g. auditing) a four-eye principle (or simultaneous evidence collection) is desirable. Many debates in CSR have focused on changes to data collection methods. Eisenhardt claims that alterations to data collection during the research project are allowed as long as the alteration is likely to better ground theory or to provide new theoretical insight. "*This flexibility is not a license to be unsystematic. It provides a controlled opportunity for researchers to take advantage of the uniqueness of a specific case and the emergence of new themes to improve resultant theory.*" With this evolving view of case study research, validity is increased, since a certain case can reveal emerging, previously undiscovered, information that is relevant to the field.

Another limitation is that single CSR is limited to one organisation. This micro level of research limits options for comparing cases or drawing generalizable conclusions [75]. We clearly require more than just one or two cases to represent an industry. Single CSR is also limited from a validity perspective. To eliminate single-case bias numerous cases are required. In a single case study knowledge transfer mostly takes place on an individual basis (unless it is published), since only a limited number of people are involved in the business environment [136]. This issue can be resolved by setting up a case evidence database in which all records and data can be stored and managed [77] and later on extracted and shared by others. Successful knowledge sharing in Information Security via web-based databases was researched by Feledi et al. [1]. Feledi encourages the use of knowledge database systems for knowledge-intensive topics.

APPLYING CASE STUDY RESEARCH IN BIS RESEARCH

In Business Information Security research there is a need to explore generic interventions. This can be done by using qualitative methods such as Delphi, Surveys or Group Support methods. Although the strength of these methods is their ability to reach out to a larger population of respondents, CSR makes it possible to dive deeper based on previously collected data. It provides us with a more in-depth understanding of the phenomena. With

numerous cases it “strengthens the results by replicating the pattern-matching ability and hereby increases confidence in the robustness of the results” [77]. In Business Information Security research the effects of intangible factors are relevant for successful engagement in the MBIS process, or for the implementation of certain controls. These intangible factors (e.g. leadership and culture) can be examined by using CSR. Extreme case studies provide more detail on specific ontological and epistemological issues observed during for example a face-to-face interview. Extreme case studies can also be used to validate artefacts or instruments (e.g. security surveys or checklist). In the case of BIS a body of knowledge can be built where there is no list of governance practices that can be used by practitioners. CSR can be used to validate such a list, together with directors or managers (people in the business environment). Within BIS research it is becoming more important to collect evidence, due to stricter regulations and auditing guidelines. CSR that encompasses systematic data collection (observations and interviews) stored in an artefact (e.g. data collection tooling) that can be validated by an auditor increases plausibility and credibility. Credibility because it provides proof of outcomes and plausibility because, due to the use of tooling, the researcher is forced to collect and store knowledge items that are relevant. This triangulation of methods where data that is gathered – observing, interviewing and documenting – is captured in a tool that includes corroboration [137].

In conclusion we can state that CSR is limited when exploring and generating generalizable data. To explore general propositions we propose the use of questionnaires. And to capture and transfer knowledge we propose GSS or surveys. These can play a role in the quest for Business Information Security Governance practices that can form a frame of reference. For practitioners we propose the use of group discussion and group prioritisation. The resulting data set can be used later on to make a deeper qualitative analysis of the findings from GSS or Delphi research. CSR can also be used to study certain intangible factors such as culture, leadership and perceptions. Within BIS research these factors play a major role in determining whether the board of directors adopts BIS and they therefore influence the success of improving MBIS. CSR can also be performed to examine the impact of certain parameters on MBIS.

2.3.5 DESIGN SCIENCE RESEARCH STRATEGY

Triangulation of methods is increasingly used *within* Design Science Research to clarify the problem, define requirements for an artefact and demonstrate whether the artefact solves that problem. “*The design-science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts* [138]. The design science strategy is about solving real-life problems. According to Johannesson and Perjons [73] DSR involves building artefacts to solve predefined business problems. “*The design science research strategy is about creating things that serve human purposes and these things are then assessed against criteria of value or utility. Rather than posing theories as in natural science, design science strives to create models, methods and implementations that are innovative and valuable* [73].

When investigating Business Information Security and the kind of problems that can arise we can distinguish two types of problems. Horst Rittel [139] refers to "wicked problems", e.g. problems that are difficult or impossible to solve (for example poverty) and "tame problems" – those that are solvable with a certain solution within a certain timeframe (e.g. involving algorithms and constructions) [73]. Conklin quotes; "*when working on wicked problems in a socially complex environment, it is much harder to notice that our tools are simply not "picking up the dirt"*" [140]. In information security, changing culture and behaviour is perceived as a wicked problem, as eighty percent of the time it is the 'human factor' that causes security incidents [23]. Understanding and getting a grip on the complexity of cybercrime is also a wicked problem. There is no 'stopping rule' that tells us when a wicked problem has been solved [141].

Johannesson and Perjons [73] state that there are problems in which the current state is viewed as truly unsatisfactory and the desirable state is seen as neutral. And there are problems where the current state is seen as neutral and the desirable state is regarded as a potentially huge improvement. Often such problems are not perceived until some innovation arises and captures people's imagination. So the term 'problem' is used to denote troublesome situations as well as promising opportunities. We follow the same reasoning in this research project and consistently use the term 'problem' to refer to an issue that can be addressed with Design Science Research.

In DSR the principle is that "*knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact. The term artefact is central to design science research and is used to describe something that is artificial, or constructed by humans, as opposed to something that occurs naturally.*" [73] Five types of artefacts can be distinguished:

- Constructs (vocabulary and symbols)
- Models (abstractions and representations)
- Methods (algorithms and practices)
- Instantiations (implemented and prototype systems)
- Design theories (improved models of design or design processes).

DSR FOR THE DESIGN AND DEVELOPMENT OF ARTEFACTS

Design Science Research (DSR) has attracted increasing interest in the Information System research domain. March and Mith initiated important DSR work with their early paper on a two-dimensional framework for research on information technology [142]. Hevner et al. [138] produced a broad framework which is used worldwide to perform and publish DS work. This framework is visualised in see Figure 11 contrasts two research paradigms in information system research: *behaviour sciences* and *design sciences*. Both domains are relevant for Business Information Security (BIS) because the first is concerned with soft aspects such as the knowledge, attitudes and capabilities required to study and solve

problems. The second is concerned with establishing and validating artefacts. To put it more precisely, Johannesson and Perjons distinguish between the design, development, presentation and evaluation of an artefact [73]. Wieringa distinguished many methods for examining numerous types of problems, e.g. design problems and knowledge problems [143]. In this BIS research project we used Hevner's work as a frame of reference for the entire DSR project and we used Wieringa's approach to address the many BIS problems that we encountered. As mentioned in Chapter 2, numerous methods are applied, mainly because BIS problems are diverse and rather complex. This is why the methods used to master them are not straightforward. Johannesson and Perjons' work delivered a research strategy for thoroughly structuring the DS research process as developing artefacts. Johannesson and Perjons also address numerous methods for examining problems and setting artefact requirements.

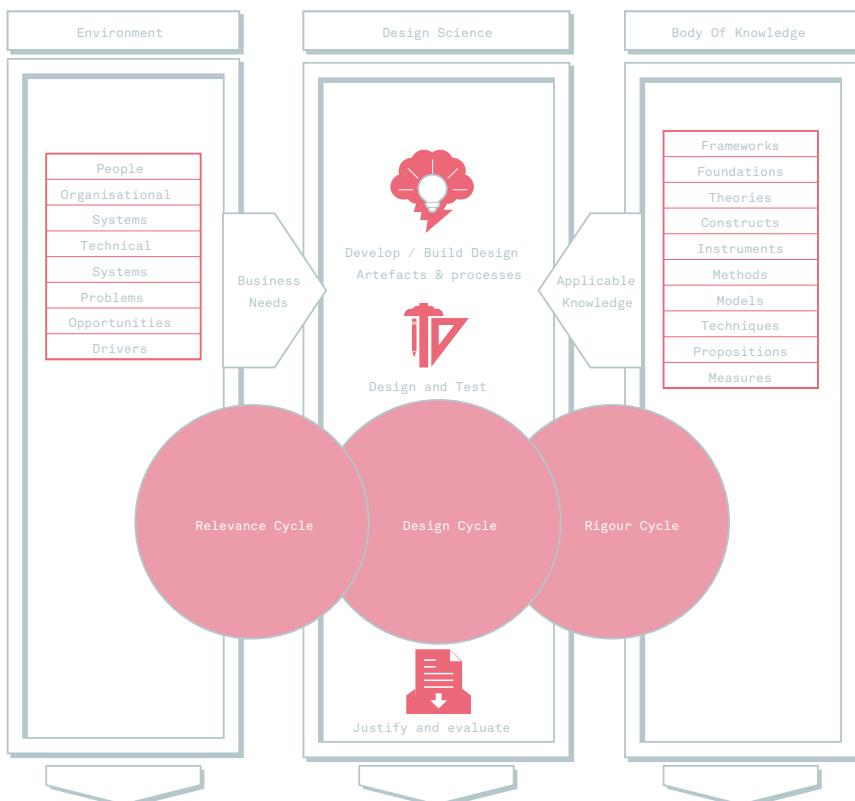


Figure 11: Hevner's Design Science Research Framework [138].

DOING DSR IN A BUSINESS ENVIRONMENT

It would be too much to expect this research project to be performed in a perfectly situated environment and in an ideal sequence. Like any other longitudinal research new insights emerged from the problems we encountered during the execution of the research. The entire project, especially the design of the artefact, was performed in a practical business environment, so it was sometimes delayed by day-to-day problems. It is therefore required to re-engineer the entire research process and map it onto the Johannesson and Perjons guidelines for designing, presenting and validating artefacts [73].

THE PROCESS OF VALORISATION

According to Hevner, DS Research is based on three major domains: the 'Knowledge base' domain, the 'Environment' domain and the 'Design Science' domain. The first is concerned with knowledge items produced and maintained with academic rigour. Theories, frameworks, models and techniques are produced in science and contribute to such rigour. These are then applied via the design science cycle to the practical environment, which includes organisations, systems and people with real-life problems. At the heart of the DS research framework is the design science cycle, which is concerned with receiving input from the knowledge base, applying this in environments and receiving feedback, in order to master problems and establish artefacts. The three cycles at the centre of the framework represent the continuous feed-forward and feedback cycles which strengthen the design and development of the artefact. The main function of this design cycle is to establish and maintain the artefact and the main purpose of the artefact is to solve problems. The process of assessing and refining the artefact requirements is necessary to continuously test the artefact for its relevance to the practical environment (mainly to solve problems) and its contribution to the academic rigour (knowledge base). Creating business value due to the application of DSR artefacts is described as valorisation.

2.3.6 USING DESIGN SCIENCE RESEARCH TO CREATE ARTEFACTS

Johannesson and Perjons state "*Design science is the scientific study and creation of artefacts as they are developed and used by people with the goal of solving practical problems of general interest. An artefact is an object made by humans with the intention to be used for addressing a practical problem.*" [73].

Wieringa distinguishes between knowledge problems and practical problems leading to differences in research questions. In his paper "Design Science as Nested Problem-Solving, the author claims; *Practical problems call for a change of the world so that it better agrees with some stakeholder goals. Knowledge problems by contrast do not call for a change the world for a change our knowledge about the world* [143]. To solve knowledge problems requires knowledge-oriented questions. Wieringa refers to "problem investigation" methods to avoid research methodology challenges and proposes a framework of guidelines for design science researchers to achieve certain goals. In his guidelines Wieringa defines the regulative cycle

as an important step after identifying the type of problem, e.g. a practical or a knowledge problem. In this regulative cycle various stakeholders are involved: architects, product managers, system engineers, etc. In this sense the regulative process is the general structure of a rational problem-solving process. The proposed guidelines are closely related to Nunamaker and Chen's [144] guidelines for system development. These authors also propose a regulative process but in contrast to Wieringa focus less on problem investigation and problem nesting. In the case of BIS this is important since we sometimes think practical problems can be solved by technology rather than by knowledge. Johannesson and Perjons also propose such a regulative process in the form of *explicating* the problem via a structured method of defining knowledge problems and design problems. In this research we follow Johannesson and Perjons's guidelines since this framework is not limited to the design of requirements but also covers demonstration and evaluation of the artefact. The BIS problem is nested in three knowledge domains. First there is a lack of awareness, which is mainly due to a lack of knowledge about the context (regulations, forces of power, influences) and how to interact and perform at a certain maturity level within this context. Second there is the problem of how to get a grip on the topic, i.e. knowledge about managerial parameters. This topic brings technological, legal, personal and financial issues into the organisation and makes it complex to monitor and manage. The last domain is knowledge, meaning and understanding (i.e. epistemology), i.e. what knowledge is and how it can be acquired, and the extent to which knowledge pertinent to any given subject or entity can be acquired. It asks the question: "*how do we know when we have done enough?*" At what level of knowledge does this end, or does it perhaps not end and can we only contribute to solving these issues by designing and establishing knowledge acquisition and sharing vehicles to address and solve these problems? The research goal in this project is to address three types of practical problems that are of general interest:

- knowledge problems
- awareness problems and
- design problems.

One limitation of DSR is the need for continuous alteration and maintenance of the artefact. Validation of the artefact, in order to execute DSR, has been attempted by numerous authors [145] and it is also seen as one of the limitations of DSR publications, since validating is hard and complex [145]. Another limitation is objectivity; this refers to the extent to which research is impartial and freed from the subjective judgement of the researcher, especially with interpretivist research such as BIS [77]. DSR is sometime limited in precision due to the absence of rigour in practical environments. The output of the research iterations largely depends on the way the problem is framed. When the input into the design science framework is insufficient or incomplete, the outcome is poor. As Johannesson and Perjons state in their book on design sciences "*The problem needs to be precisely formulated and justified by showing that it is significant for some practice. The problem should be of general interest, i.e. significant...*" [73]. This identification and explication process within BIS research

would ideally come from literature, GSS and/or Delphi research methods. In Figure 12 the DSR steps in the framework are visualised.

Artefacts are developed, tested and validated through the use of the design science frameworks such as those used by Johannesson and Perjons [73], Wieringa [146] and Hevner in 2004 [138]; see Figure 11. In Hevner et al. [138] on the right is a representation of the theoretical knowledge base that provides the materials through which design science is accomplished. This Body of Knowledge consists of prior established frameworks, foundations, theories or constructs. The knowledge base in fact establishes the academic rigour of the design sciences. On the left side the practical business environment is represented. This defines the problem space in which the topic and its related problems arise. The environment encompasses people, organisational systems (structures, processes and relational mechanisms), technology, etc. and confirms the relevance of design science. In the centre of the framework the design science artefact is crafted by process activities related to designing, building, developing and evaluating an artefact that meets an identified business need. As a follow-up to Hevner's work Johannesson and Perjons present seven DSR guidelines [73] – guidelines that can assist researchers in understanding the requirements for effective DSR. Although design science is mainly focused on the artefact and not primarily on the execution of procedural steps, these structured steps offer strict guidance during the artefact establishment phases and I therefore propose to use the framework developed by Johannesson and Perjons for this research project.

2.3.7 RELEVANT METHODS AND TECHNIQUES FOR THIS RESEARCH PROJECT

Considering the assumptions and methodological aspects of this research, an iterative process of qualitative research methods is proposed based on the following arguments:

Literature research is proposed to '*construct validity*' based on previous academic research in the field. This includes concepts, propositions and theories within a certain subject or about a certain object. This first step is essential due to the complexity and multiplicity of the BIS domain. It also helps structure thinking.

Group Support Systems (GSS) research to validate and prioritise elements within the topic and to establish a common ground of awareness and knowledge (also to overcome epistemological challenges). The aim is to achieve consensus on the urgency of the topic. GSS in relation to transformation processes is proposed as an instrument to enable decision-making in groups (e.g. by management teams or Boards of Directors (BoD)). To encourage boards to get out of an ad-hoc mode and adopt a continuous process thinking mode. After prioritising certain items, the next step is to facilitate the decision-making process, for example in strategy sessions among BoDs or management teams. GSS also captures and records findings during the research and decision-making, which enables knowledge management (generating, sharing and transferring knowledge). GSS can also be used as an

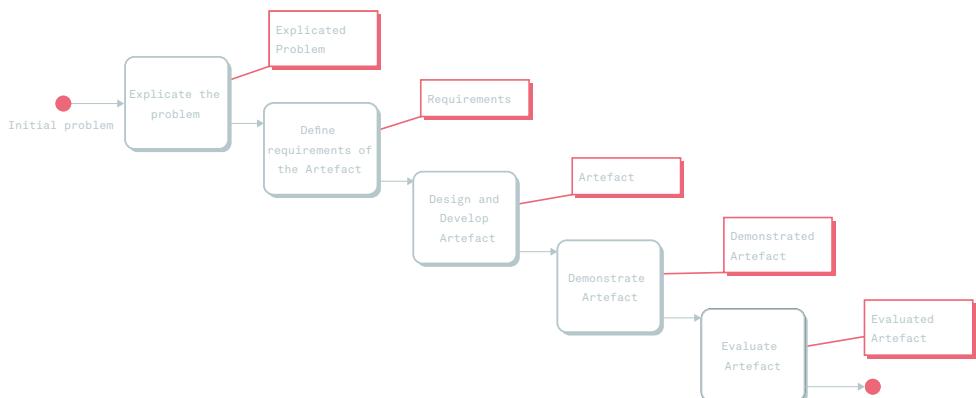


Figure 12: Overview of the framework for design science research [73].

instrument for carrying out Delphi research [106] and thus across geographical distances without group interference and with some degree of anonymity [106]. In this research project we position GSS research as referring to groups such as boards, stakeholders and users. It facilitates a research method that encourages discussion and group thinking. GSS research is also proposed as a qualitative research method for generating and prioritising artefact requirements [147].

The Delphi research method is proposed to establish new questionnaires or to revise existing ones without group interference, for example ISO/NIST/ISF⁴ questionnaires. It establishes a broad view on a topic and can be used to express either quantitative or qualitative views, for example generic factors that can influence the MBIS process. These include leadership, culture and knowledge. Due to web-based techniques the Delphi method can include numerous international expert respondents if needed. Delphi, which involves numerous iterations to review previously collected data, is proposed for expert groups but it is limited within companies where the objective is to collaborate and debate. Data can be generalizable at the macro level (across sections, industries, regions and jurisdictions, etc.). Delphi is proposed in BIS research to set requirements for establishing, re-evaluating and maintaining the artefact.

Case study research as a field testing technique within the relevance cycle in DSR is proposed for gaining deeper insights and to explore or explain certain viewpoints [77] once GSS research has already taken place. Using earlier findings gained in previous qualitative studies, it allows us to dive deeply into certain company-specific topics. Although CSR is limited in terms of the number of cases, examining extreme cases can provide more in-depth knowledge on intangible factors that influence MBIS and how these factors

4 Numerous practitioner communities produce interview templates, questionnaires, surveys and best practices.

manifest themselves. CSR can also be used to compare certain practices between one or two industries. CSR is particularly valuable in BIS for validating previously collected data. This is increasingly required by regulators and auditors.

In conclusion we assume that ontological and epistemological objectives can be addressed by using these mixed methods of qualitative research and the iterative process of ensuring academic rigour and practical relevance. A qualitative research method such as GSS can facilitate both acquiring and sharing knowledge and it can help explain the problem. GSS can be a useful follow-up to literature research, to gain consensus about certain concepts and to encourage group thinking. Whenever it's possible to use knowledge thus and to share it in the decision-making process, GSS uses that phase of the research as well, which makes it suitable for addressing problems and turning them into actionable items in a business environment. GSS can also facilitate the creative process of setting functional requirements for a design science research artefact [147], i.e. indicators of the individual maturity level. The Delphi research method (using surveys) would ideally be positioned parallel to or before GSS to scrutinise or validate specific content in the literature. According to Tremblay [147], validation through expert opinions (in focus groups) would enhance the academic rigour as well as the relevance of research and contribute to a knowledge base. Case studies can deliver valuable data on intangible factors of influence that Delphi or GSS cannot externalise. CSR can be used to evaluate and test the artefact. This is visualised in Figure 13.

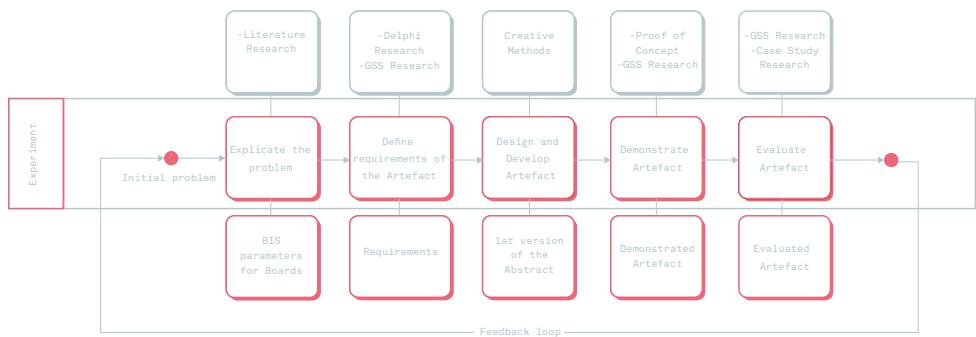


Figure 13: Multi-methods used in DSR, based on the Johannesson and Perjons framework [73].

2.4 PROPOSED MULTI-METHOD APPROACH

Numerous methods are examined, based on the literature, for designing and engineering a BIS artefact. The core contribution of these methods, which are used in combination with DSR, is summarised in Table 1.

Table 1: Research methods and their contribution to BIS research.

TYPE OF RESEARCH WITHIN DSR	Contribution to designing and engineering a BIS artefact to support the analytical work
1. LITERATURE RESEARCH	Explicating and defining the problem in a systematic, structured way. Objectivity removes Fear Uncertainty and Doubt (FUD). Providing an unbiased, structured point of departure for the design cycle. Requires a certain level of expertise in the topic.
2. DELPHI RESEARCH	Providing an anonymous inventory and selection of views and standpoints (preferably based on data in the literature). Rigorous examination process for scrutinising the problem via, for example, expert opinions. Collecting global views on criteria requirements with the use of technology. Knowledge sharing. Enables double loop learning [148] via numerous iterations. Automated. No geographical limitations. Limited in group interaction and discussion.
3. CASE STUDY RESEARCH (CSR)	Deeper qualitative insight into BIS parameters and requirements within a certain industry/country. Used for confirmatory and exploratory studies related to validating requirements. Detailed insight into the effectiveness of requirements (i.e. critical success factors). Supports retrospective approaches. The personal approach encourages the target group (Boards of Directors) to engage in BIS. CSR is time-intensive.
4. GROUP SUPPORT SYSTEM RESEARCH	Makes creating, sharing and capturing knowledge possible as well as discussion of design items. Stimulates design thinking and stakeholder collaboration due to the 'group element'. Provides an ability to collect, assess and select product requirements in a very short timeframe. Supports the regulative process [146] of testing and validating requirements. Processing large data sets. Double Loop learning [148]. Bridging knowing-doing gaps. Stimulating group dialogues (i.e. among Boards of Directors and Management teams). Makes it possible to establish group consensus. Supports the decision-making process. Threat of the 'law of the decibel'. Requires professional group moderation skills [149].

The proposed research method starts with the initial phase of rigorous literature research (1) to explicate the problem and this is followed by Delphi Research (2) to predefine views and standpoints and further explicate the problem via numerous views and iterations. After that, Case Study Research (CSR; 3) provides in-depth knowledge and data on certain influences on BIS such as context, regulations, technology and culture.

The data gathered during Delphi and CSR is used in GSS to support collaboration and improve the decision-making. GSS can also be applied to determine the requirements among stakeholders and to prepare or guide the stakeholder-user group in discussing the implementation (making it fit for purpose).

The aim of this research was to define parameters of control using qualitative research methods, with the potential opportunity of setting requirements for the initial experimental development phase of the design artefact that does the administrative work. When the qualitative approach is further evolved via the rigour and relevance cycles and data from the environment is entered into the artefact, it becomes a knowledge base, allowing quantitative analysis on the data gathered. In Figure 14 the continuous improvement cycle of BIS is divided and detailed per PDCA step towards collaboration and administration (collaboration to gain consensus and administration to capture and report the BIS status).

The following chapters (4, 5, 6 and 7) all use GSS as a multi-method research technique as a collaboration tool with the objective of examining potential artefact requirements and exchanging knowledge.

QUALITY ASSURANCE WITHIN THE PROPOSED METHOD

The proposed method of qualitative interpretivist research inherently has some risks. To avoid any influence of the researcher e.g. based on personal biases towards the research results, the following mitigating mechanisms have been used. These mechanisms are designed to secure the objectivity (independence), reproducibility, precision and transparency of the research work:

- Apply the DSR framework proposed by Johannesson and Perjons [73]. This framework prescribes clear steps and criteria throughout the artefact development process.
- Make use of numerous participants from a wide variety of organisations/professions.
- Record the GSS sessions and demonstrations on video and/or audio.
- Publish the – intermediate – research work in peer-reviewed-journals and at conferences.
- Document all sessions (GSS meeting reporting) as well as the artefact development process (e.g. via change logs, version documentation, backlogs, etc.).
- Use an external professional moderator during the GSS sessions.

These activities and mechanisms, which should ensure objective, precise and reproducible research, are included in the appendices.

Figure 15 displays the methods applied in the several phases of the research, in order to provide answers to the research questions.

2.5 RESEARCH ASSUMPTIONS

The research propositions presented in Chapter 1 provide the basis for examining the BIS topic. In order to determine whether the building blocks of the research project i.e. the factors (variables, constructs, concepts) are comprehensive (are all relevant factors included?) and parsimonious (can we leave out factors since they add little value to the understanding or are similar to others?) [150], we denote each factor that has an influence

on the theoretical construct. The objective here is to define clear requirements and assumptions to

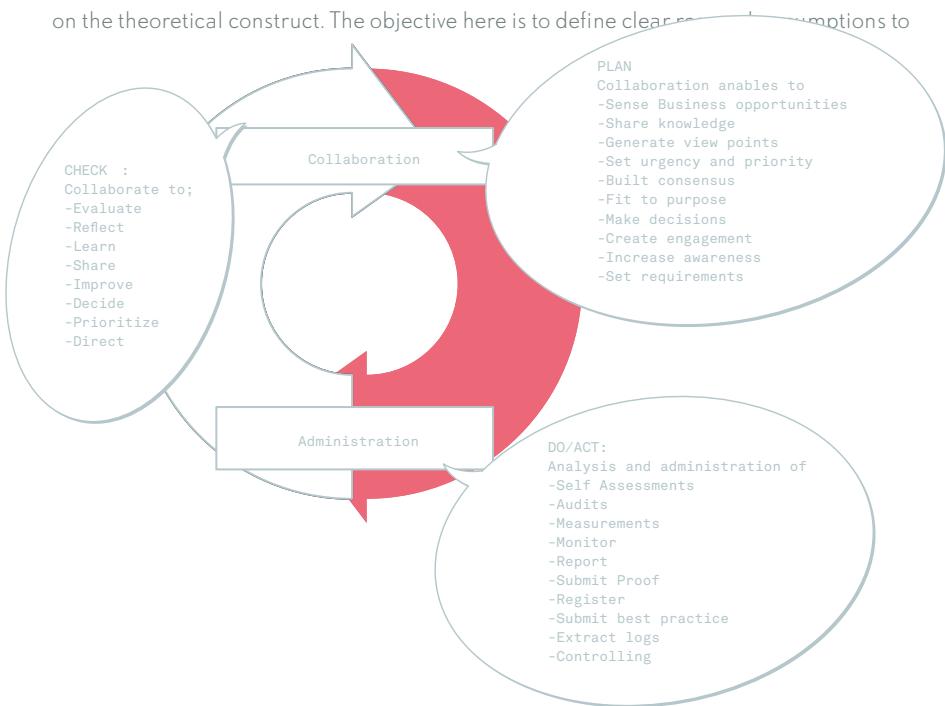


Figure 14: Proposed method and PDCA-based activities used to improve the maturity of BIS.

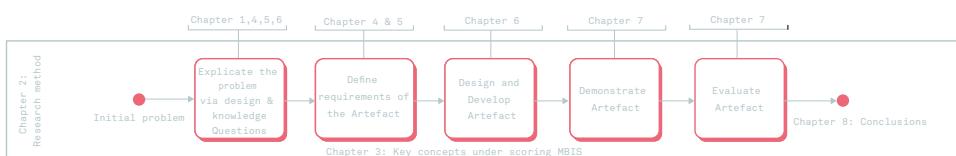


Figure 15: Thesis structure, based on the DSR Framework of Johannesson and Perjons [73].

take into consideration during the research project. The research methodology propositions also provide the foundation for examining the contributing factors that enable the BIS maturing process.

In line with Whetten [150], the theoretical construction of the research project and therefore its theoretical contribution lies in the questions "what", "how", "why", "who", "where" and "when."

The grey boxes represent the *what* of our theory, providing the construct that we need to consider to help explain an organisation and its context. These constructs consists of numerous elements and are enumerated in the next section in Figure 16.

The scope and context of the organisation differ and these two constructs are therefore situational. In terms of the **context** we answer the question "*Who do I need to do this for?*" (e.g. stakeholders), while **scope** answers the question "*What do we need to do?*" Elements of the context are shareholders' objectives, geographical location, geopolitics [46], jurisdiction, etc. Elements of the scope are regulations, corporate social responsibility norms and certain business restrictions. Both are considered to be external forces that influence the organisation and the transformation process (represented by the dotted arrow), e.g. the maturing process.

The various elements are categorised under three major constructs:

- The construct of **Management and organisation** relates to all elements that formalise the structure and the processes within the organisation, from policy formulation to operationalisation.
- The **resource capabilities** relate to the internal competences and skills employees can use to put strategic plans into operation. Usually we refer to the processing power of the organisation needed to bring about changes. This concept is directly related to the scope. Thus, *what we need to do* in order to mature must be achieved with internal resources.
- The **culture** of the organisation relates to attitudes and behaviour to BIS and therefore the willingness to engage into a maturing process. As Peter Drucker put it, "*Culture eats strategy for breakfast.*" This key assumption has considerable effect on the success of the maturing process [7].

These three internal constructs address the *what* question stated by Whetten [150]. The lines and arrows in the figure above represent the *how* question, i.e. how the constructs relate to each other.

Whetten [150] also refers to the "who, where and when" questions. These relate to limitations to the propositions generated from a theoretical model. Since the BIS phenomenon is embryonic, it is very hard to predefine limitations upfront. The major question *who is*

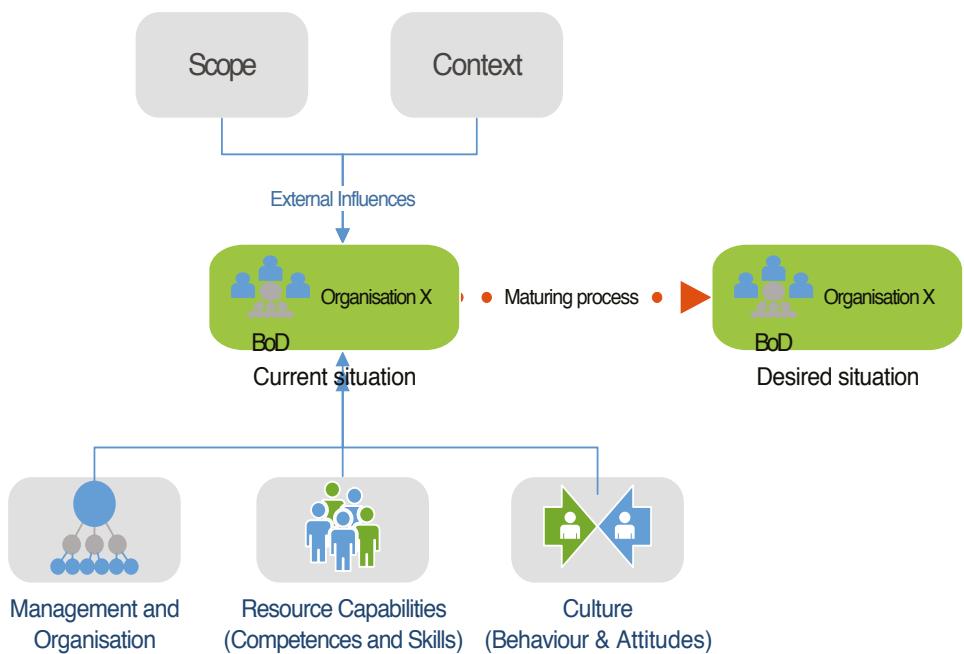


Figure 16: Denoting the why, what and how, from Whetten [150], in relation to MBIS research.

indicated by the green box and the dotted red arrow. It shows that we focus on exploring parameters that organisations can apply in order to mature (from the current to the desired situation). It is also important to highlight the fact that this research only focuses on governance and executive management (strategic level) practices. The *where* question relates to the fact that this research project is performed with Dutch organisations and in collaboration with Dutch respondents. This might limit the generalisability of the data gathered to Dutch industry. The major assumption behind this research was that there is a limited direct relationship between the individual constructs. Usually events occur and have a positive or negative effect on the change process. This might be by coincidence or on purpose, but usually this is not a rational or visible event. A combination of events can enable the maturing process. So we refer to preconditions, barriers and critical success factors, all predefined items that strongly influence the success of the BIS maturing process.

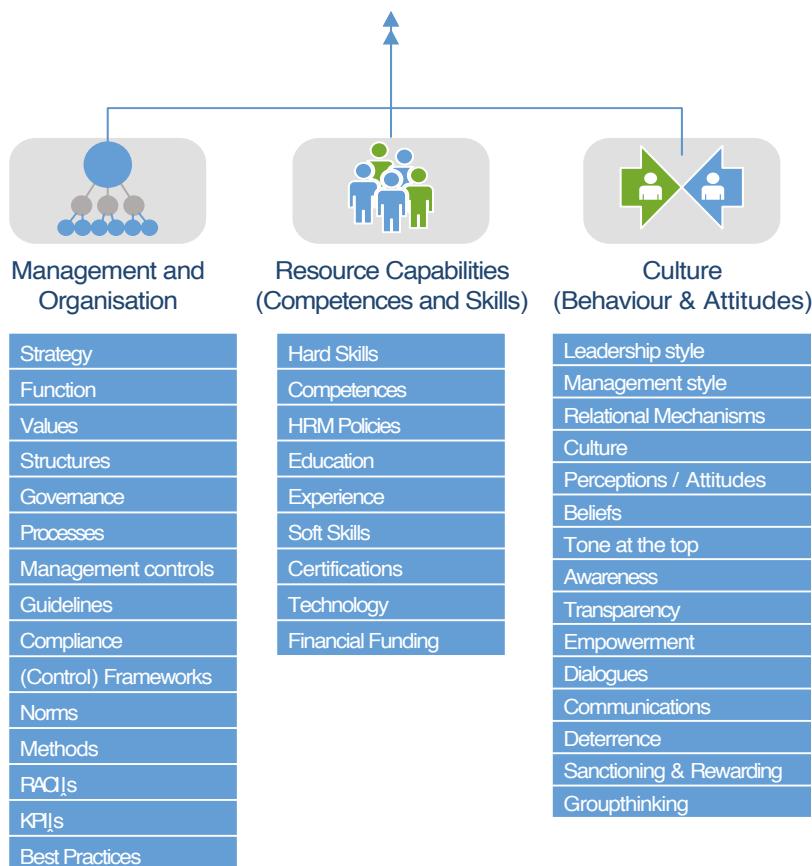


Figure 17: Enumeration of the theoretical constructs.

3

DEFINING KEY CONCEPTS OF BUSINESS INFORMATION SECURITY

3.1 INTRODUCTION

In this chapter key concepts that relate to BIS are addressed. It is not the intention to be exhaustive since BIS is a broad domain. Only the concepts that have relevance in getting answers to the research questions are detailed in this chapter and form the ingredients for the conceptual framework suggested in chapter 1.

Key concepts underscoring the topic of Business Information Security and the problem area are visualised in the diagram below. This starts with the main business orientation, which is to deliver services to customers, with the support of IT services. These services are established with IT components, including IT security services. Besides IT services business organisations are supported by numerous other support functions such as HRM, legal, risk management, etc. In past decades the Chief Information Security Officer (CISO) has focused on the IT elements [151]. Due to human error, regulations and cyber-attacks, this CISO role has now changed into a more business-oriented discipline, which increasingly involves strategic planning [25]. This relates to the "resource-based view of the firm" theory (RBV) [152] in which organisational excellent performance and successful transformations rely on the capabilities of the resources that are involved in strategic planning. These resources are increasingly influenced by, e.g. human error, regulations and cyber-attacks and therefore indirectly influence the task and knowledge requirements of the CISO. Within the RBV of the firm theory, knowledge refers to these resource characteristics [153], [154]. In the section below the changing role of the CISO is elaborated in more detail. In relative smaller organisations the role of the CISO is not a dedicated function but a combination of responsibilities within the function of the Chief Information Officer, IT Director, or Chief Technology Officer. Since this research project focuses on the strategic level within mid-market organisations we do not hypothesise that there is necessarily a dedicated CISO-position.

3.1.1 INFORMATION RISK AND SECURITY MANAGEMENT

In recent decades IT security has become 'information security' [61]. ISO specifies information security as "*protecting information assets from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investment and business opportunities*" [155], [156], [94].

The core principles for information security are confidentiality, integrity and availability, which are usually referred to with the acronym CIA [155], [157].

- **Confidentiality** means preventing disclosure of information to unauthorised parties.
- **Integrity** seeks to prevent unauthorised modification of information.
- **Availability** is the term for all kind of ways to make necessary information available to users within an enterprise and within the 'extended enterprise'.

In addition ISO added other properties such as authenticity, accountability, non-repudiation⁵, reliability, and auditability due to audit and compliance regulations. Thus Information Security deals with assurance of a certain level of system quality [158]. Information security is directly related to information risk management. Many authors have performed research into risk management models and methods such as CRAMM⁶, OCTAVE, [159], NIST, [160] and ISFs' IRAM [161], particularly into risk analysis and risk assessments in order to analyse threats, vulnerabilities and the impact on information systems and derive controls for mitigation. To determine the information security requirements, e.g. controls in the form of process controls, technical controls or people controls is based on the risk and impact estimation on the critical business assets.

THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer's role (CISO) was introduced as a response to the emerging domain of Information Security. The role of the CISO has emerged from a pure IT-oriented role to become a strategic boardroom advisory role [25] "*The CISO is generally the "heart and soul" of an information security program in most organisations. There is no better way to obtain a pulse regarding cyber risk*" according to The Institute of Internal Auditors (IIA) [162]. The CISO "*defines the information security strategy and organises and manages the organisation's information security in line with the organisation's needs and risk appetite*", according to the European Competence Framework [163]. This framework prescribes clear directives for the role of the CISO as well as the required skill set. Numerous reports emphasise the importance of the CISO role in having an effect on Information Security strategy formulation and implementation. IT Policy Compliance Group reports that firms that standardise procedures and controls for IS and manage IS via a dedicated IS staff which is led by a CISO achieve 8.5% higher revenue than industry averages (n= 3000 organisations) [164]. This report also reveals that benchmarks conducted during the past year show that one of the key factors influencing outcomes related to the loss or theft of customer data is whether a Chief Information Security Officer (CISO) is in charge of the information security and assurance function of the organisation. In 2015 Accenture [165] did research⁷ into so-called 'leapfrog' companies that outperform in the field of Information Security compared to others, for example, due to the positioning of the CISO as a strategic role [165], [166]. "*These relatively new aspects of the role require CISOs to be successful change agents. To do this they need to be able to reflect on, and understand, the impact of their role on organisational culture*" [25] The role of the CISO is that of a strategic board adviser, were as Hooper et al. states "*organisations need to embrace their concern about cybersecurity and build it into their selection criteria for board members*" [25].

- 5 ISO 2.54: The ability to prove the occurrence of a claimed event or action and its originating entities.
- 6 CRAMM (CCTA Risk Analysis and Management Method) is a risk management methodology, currently in its fifth version, CRAMM Version 5.0. (source Wikipedia)
- 7 A total of 247 companies participated in this study, which was performed by Accenture in collaboration with Ponemon Institute.

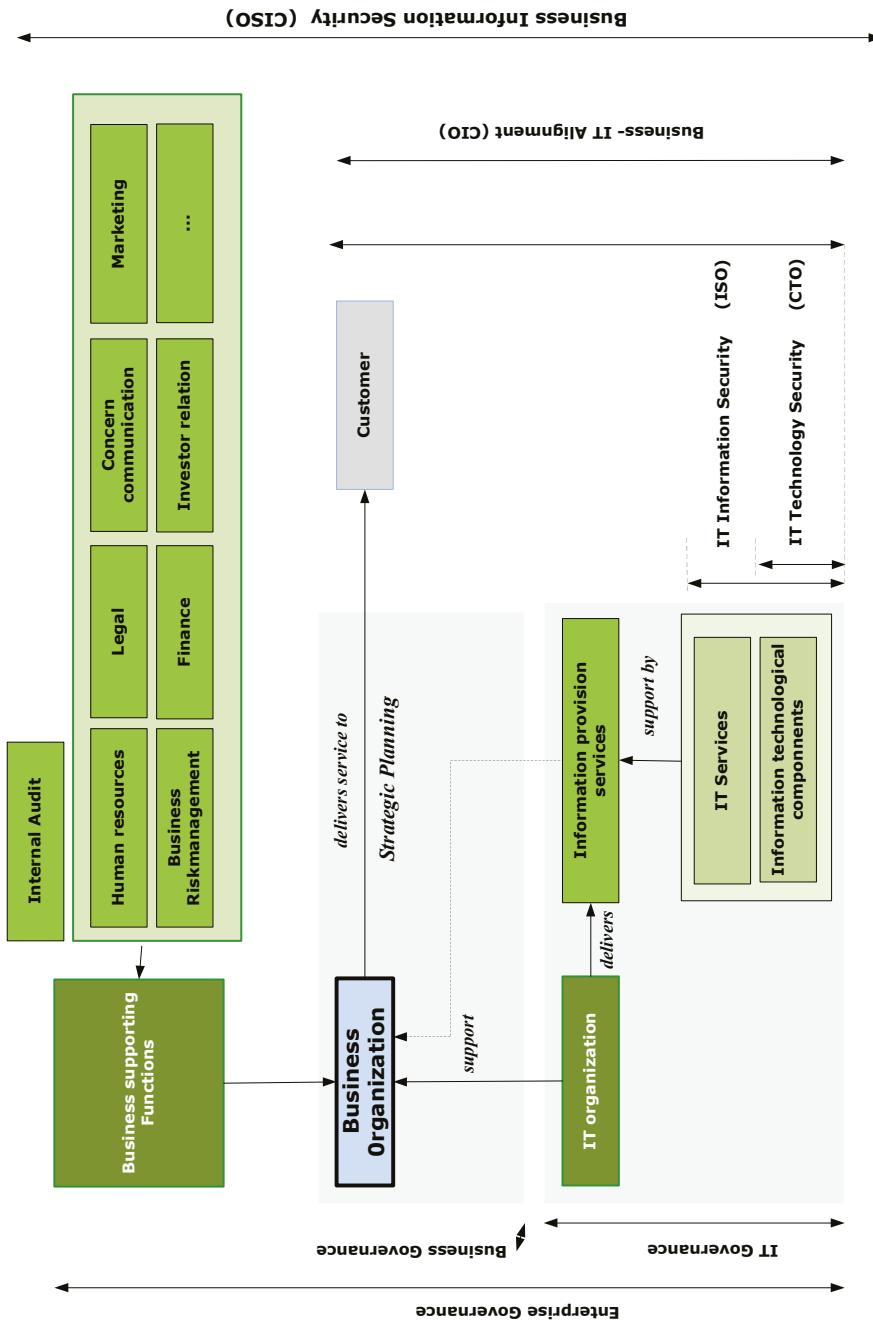


Figure 18: Conceptual model of the BIS domain.

Various authors address the importance of the role of the CISO into balancing the responsibilities of risk and security into the first, second and third line. In 2012, The IIA proposed the three lines of defence concept to assist organisations govern enterprise risks and help executives understand the topic without confusion. If an organisation has an effective governance model, the second line of defence is responsible for performing most of the governance functions related to Business Information Security. According to IIA this role is headed by the CISO, who defines the policies, standards, and minimum technical configuration standards [162]. This concept is frequently examined and published by numerous bodies, such as COSO [167], ISACA [168] [169] and Forrester [166]. The main concepts of this "three lines of defence" concept are;

The **first line** of defence has line management oversight and is mainly the IT operations function and the "business". This first line implements the policies and standards and is responsible for monitoring of the networks and infrastructure. The first line is also responsible for the workforce awareness and behaviour. The first line has process controls in place (e.g. encryption, anti-malware, data leakage prevention) and mechanisms in place to test the effectiveness of the controls (e.g. least privileged, segregation of duties etc.). In the **second line** of defence the CISO Office, according to Forrester [166], is responsible for governing those tasks and ensuring that the appropriate monitoring, reporting, and tracking of key controls is being performed by IT operations. In this second line also risk management, financial control, quality management, compliance, threat intelligence and brand monitoring is taking place. This second line reports to the board or senior management. Since the role of the CISO is becoming increasingly important to IT enabled companies the IIA states; *"The board must ensure that the CISO is reporting at the appropriate levels within the organisation. Keep in mind that, although many CISOs continue to report within the IT organisation, sometimes the agenda of the chief information officer (CIO) is in conflict with that of the CISO. As such, the trend has been to migrate reporting lines to other officers, including the general counsel, the chief operating officer (COO), the chief risk officer (CRO), or even the chief executive officer (CEO), depending on the industry and the organisation's dependency on technology [162].* Finally the **third line** of defence, internal audit, reviews the first and second line to ensure that the controls are effective, have suitable coverage, are deployed consistently and are proofed with evidence. So the external auditor and regulators can perform their external duties. Recently the IIA and COSO collaborated into a examining the main principles to consider for the CISO when navigating between the first, second and third line of defence.

3.1.2 BUSINESS INFORMATION SECURITY MATURITY & ALIGNMENT

Information risk and security management within organisations evolves in a similar way to organisational growth and development. An important growth model that can be used to identify the several stages of growth was developed by Larry Greiner [170]. It identifies two phases: *growth and crisis*. According to the Greiner Model, each phase of growth implies

a phase of crisis. Examples of crises include those related to leadership, simply because a start-up requires another type of leadership than a company that is scaling up. The larger the company gets, the more it depends on coordination and collaboration. This is especially the case when a company lacks clear boundaries due to extended networks, internet or electronic interfaces (e.g. XBRL⁸). Phase 5 implies a process of continuous collaboration and improvement. Greiner refers to a sixth phase that suggests that "*growth may continue through merger, outsourcing, networks and other solutions involving other companies*". Each phase of organisational growth and the current state it is in also influences the level of BIS maturity.

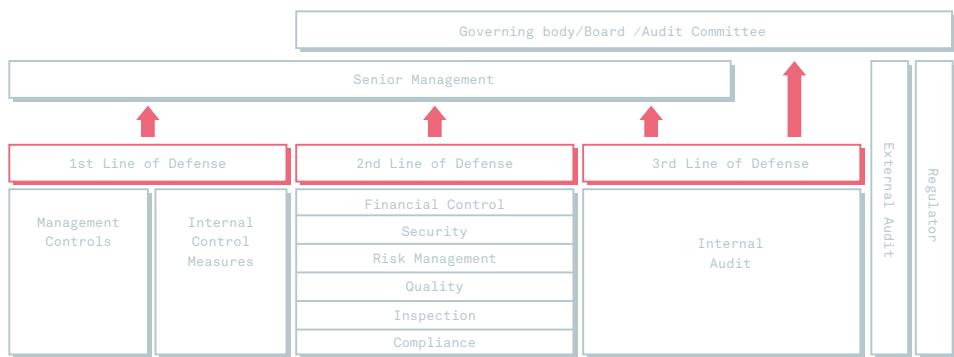


Figure 19: Three lines of defence concept taken from the IIA report from 2013 [162].

Ferraiolo and Sachs [171] refer to maturity models as models that can be used to measure an organisation's current state of information security maturity, irrespective of industry type and organisational size. In this context, maturity implies a potential for growth in capability and indicates both the richness of an organisation's security process and the consistency with which it is applied in projects throughout the organisation.

To express a company's security maturity in the form of a number we refer to COBIT4.1. This method was extracted from the Capability and Maturity Model (CMM) developed by the Systems Security Engineering Institute at Carnegie Mellon University (SSE-CMM, 2003) [172]. CMM is mainly used to make a snapshot of the current situation to determine what is missing in order to attain the next maturity level. CMM is an important predecessor of other maturity models that are used in information security, such as Citigroup's Information Security Evaluation Model (CITI-ISEM)³, COBIT® Maturity Model 4, Gartner's Security Maturity Model, Stacey's Security maturity Grid and many others. We highlight the most relevant ones for this research project, either because they have a direct or indirect relationship to BIS or reveal certain limitations that we need to consider during this research project.

⁸ XBRL (eXtensible Business Reporting Language) is a freely available, XML-based global standard for exchanging business information that is used to define and exchange financial information.

Smit [173] researched the levels of business continuity management (BCM) maturity levels and why organisations first need insight into their BCM state before they can develop a BCM strategy to reach the next maturity level. She developed a model based on the BCM theory instead of looking at existing models. Smit integrates security management into BCM and makes it an integral part of the model. Smit concentrates on building a practical model rather than looking at actual applicability in practice. She did not include real-life testing of her model, leaving that to future research.

Chapin and Akridge [174] studied information security metrics in order to measure and then improve their incorporation into a continuous Total Quality Management (TQM) process. They adopted the ISO17799 (now ISO27001) standard to develop a complete security programme (the Security Program Maturity Model), which involves a large number of security elements (10 ISO elements) that would eventually provide insight into the state of security maturity. This study, which was adopted and published by ISACA (Information Systems Audit and Control Association), is a good example of making maturity measurement practical for large as well as mid-market organisations. However, practical testing and validation of the method is still needed.

AlAboodi [175] studied the existing models of the Code of Practice (BS7799) in combination with his self-developed maturity model. The author did not explain the measurement of the level and the granularity of interventions per maturity level in detail. This study is limited as it excludes practical research and validation within organisations (and their environment).

El Aoufi [22] did action research with the COBIT 4.1 maturity model within several organisations. He applied the model first to demonstrate a common language and apply frame of reference to the business as well as the security departments. In later research he presented the required controls in order to maintain this security level. Each security intervention in place in these organisations was then assessed based on this model. It seems wise to adopt this way of working in order to ensure not only that the maturity model way of working is accepted but also to achieve consensus and mandate future steps on the individual controls (e.g. interventions).

In 2014 Tewarie conducted PhD research on principle-based auditing and the necessity of structuring the Term of Reference (ToR) for auditing [176]. Tewarie developed a maturity model framed as the Information Security Object Maturity Model (under development and still to be published). This model preserves scope for decomposing in detail each maturity level requirement per object and revealing the relationship between the maturity levels. This model requires additional empirical validation.

Ferraiolo and Sachs [171] define maturity level as: "*A well-defined evolutionary plateau on the path towards becoming a mature information security within the organisation*". Each level

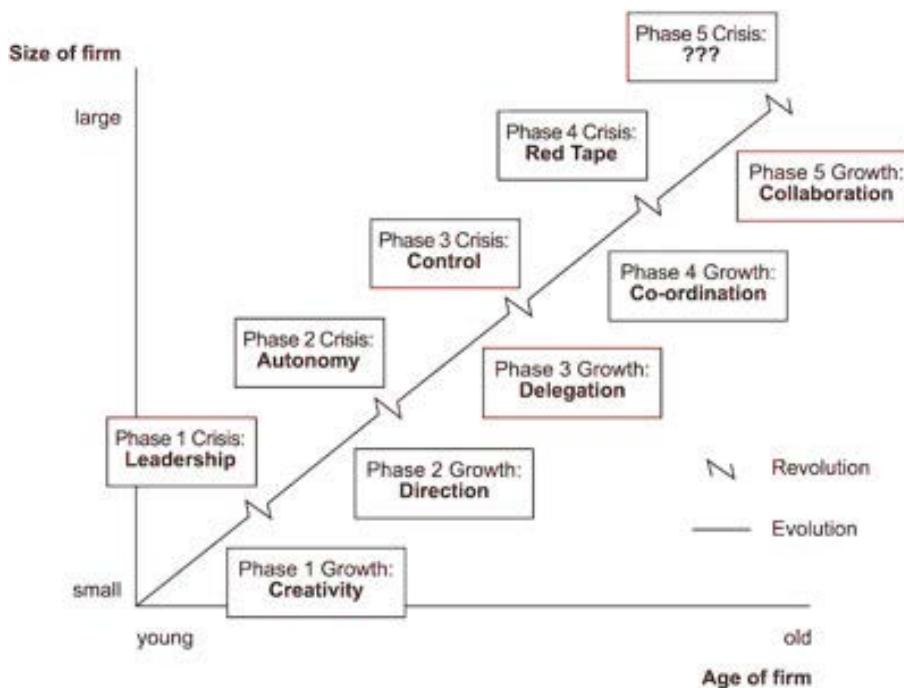


Figure 20: Greiner's growth model defines five stages of growth taken from Greiner [170].

provides a step in continuous security process improvement. Each level then provides the foundation for improvements undertaken to reach the next level.

Most of the above-listed information security maturity models provided by academics (Smit, Chapin & Akridge, AlAboodi, Tewarie, etc.) lack practical validation in the business environment. Empirical validation of IS methods and models was also acknowledged in Siponen's research work [61]. These models are therefore limited in their feedback in terms of the rigour – in the form of publications – of the empirical application of the model. In his 2005 research paper Siponen emphasised that future work on Information System Security (ISS) should move towards a more social and adaptable (empirically grounded) ISS method. On the contrary, the generic CMM model developed at Carnegie Mellon University is one of the most popular models due to its continuous sponsorship and improvements by the Department of Defence and successful adoption in IT governance models such as COBIT [177].

Maturity models provided by practitioner communities such as ISO/IEC, Gartner [178], NIST, etc. are widely adopted and accepted. In general, the number of levels in the maturity model varies, as well as the criteria per level. It is the detailing of the criteria and

requirements per level that determines the quality and applicability of the model. Originally the ISO15504 provided freedom in criteria per level in order to determine the software process improvement and capability determination. This model was later revised to use it into other areas and to create more freedom in its applicability. This freedom is also desirable within information security, especially when measuring numerous areas of improvement, e.g. the entire organisation, the software security lifecycle, the security of the network, etc. The ISO15504 did not gain a similar adoption as the CMMI model. This CMMI model remains popular in the IT, software and security areas, due to the fact that it was one of the first models and through its sponsorship by the US Department of Defence [179]. Another relevant model which was established due to intensive collaboration among software vendors is the "The Building Security in Maturity Model" (BSIMM)⁹ for software security [180]. Due to its extensive use by practitioners the popularity is increasing rapidly.

THE CONCEPT OF BUSINESS INFORMATION SECURITY PROCESSES AND DATA (IN DETAIL)

In the visual in Figure 21 show the key elements of information risk, security and compliance are highlighted. The information security strategy forms the input for the Information security planning. The scope of information security risk and security is determined based on reference models and standards prescribed by numerous bodies or regulators. Depending on the type of industry a company is in. The policies and standards determine the risk appetite of the organisation which is formalised in the risk management process of; risk identification, registration, treatment and acceptance. All security requirements that are needed to keep risk within the risk appetite boundaries are stored in repositories and documents. Within the IT operations numerous security process and service management processes are active in order to maintain a certain level of operational security control on the information risks that arise. All these processes are input on the performance management of information risk and security management. Selecting the appropriate parameters that reflect the relevant operational data for the right audience is a cumbersome task. A continuous measurement and reporting on the performance of the risk and security processes is needed in order for boards and executive management to maintain control over the Business Information Security maturity levels. In this visual the grey areas represent the scope of this research.

9 The Building Security In Maturity Model (BSIMM) is the result of a multi-year study of real-world software security initiatives. The model is built directly from data observed in sixty-seven software security initiatives, from firms including Adobe, Aetna, Bank of America, Box, Capital One, Citi, Comerica Bank, EMC, Epsilon, F-Secure, Fannie Mae, Fidelity, Goldman Sachs, HSBC, Intel, Intuit, JPMorgan Chase & Co., Lender Processing Services Inc., Marks and Spencer, Mashery, McAfee, McKesson, Microsoft, NetSuite, Neustar, Nokia, Nokia Siemens Networks, PayPal, Pearson Learning Technologies, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, TomTom, Vanguard, Visa, VMware, Wells Fargo, and Zynga. The BSIMM is a yardstick for measuring software security.

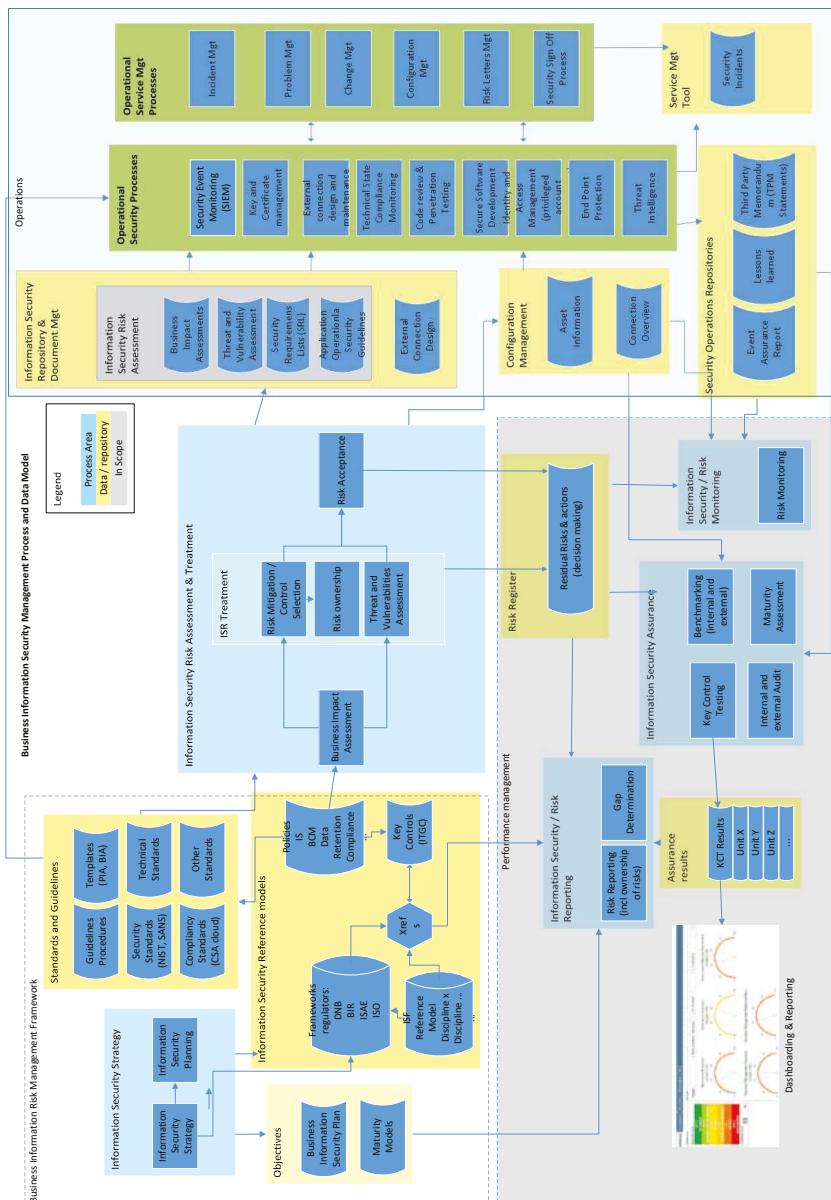


Figure 21: Business Information Security Management Meta Model

3.1.3 BUSINESS INFORMATION SECURITY ALIGNMENT

Business processes rely greatly on IT systems and technologies. Parallel to complying with expanding legislation, organisations have to cope with the rise of dynamic but complex technologies. These emerging – and sometimes embryonic – technologies, Internet of Things, domotica, social networks and the threats they pose [181] cause new headaches for business leaders. This is especially the case because these new technologies interconnect¹⁰ more and more with extended enterprise and core business applications. The possible exploitation of vulnerabilities within technologies is 'generally' covered by the vendor, either in the form of lab testing by certification bodies¹¹ or by 'security' related functionalities that need to be configured and customised. The complexity of connecting several actors (authentication of actor, authorisation of actor, administration of actor) on several information layers with a wide variety of complex protocols is increasingly subject to human error [182]. Large enterprises, government departments and multinationals seem to cope better with security challenges due to the application of adequate frameworks, methods and best practices [183].

Smaller so-called mid-market organisations do not have sufficient resources [4] and some companies lack sufficient knowledge about frameworks to successfully align the business goals to security programmes [184]. ISACA¹² put great effort into applying the SABSA¹³ framework into the COBITs¹⁴ framework, with the objective of aligning strategic goals to operational architecture requirements. In 2008 I have did empirical research on applying DEMO¹⁵ and the Enterprise frameworks to Information Security architecture principles in order to align the business to the information security function [185]. Previous Alignment studies [109] and Alignment assessment models were used to measure performance.

An important contribution was made by Luftman [186] and later on by other researchers [187], [188]. COBIT 4.1 did the initiation in measuring the maturity level of Business and IT alignment, which was later adopted by the security community in order to measure the level of security maturity alignment [22].

3.1.3 CONTINUOUS IMPROVEMENT

In this thesis we refer to maturity as the process an organisation undertakes while moving towards the desired state of control in protecting critical assets. The objective is to provide analysis and insight, based on a maturity model, in the current state, and to provide analysis and insights into the capabilities and requirements for the desired state. It is not my intention to examine the numerous security maturity models, but to provide freedom of movement

10 Interconnect can for example be portals, collaboration software such as Google docs or Office live. Or social variants such as Instant Messaging, iTunes music sharing etc.

11 Bodies such as: NIST, National Institute of Standards and Technology. ICSA labs, Consortium Operations, Security Product Testing, and Certification Programs. FIPS, Federal Information Processing Standard, CC, Common Criteria for Information Technology Security Evaluation. EAL, Evaluation Assurance Level of an IT product or system, is a numerical grade assigned following the completion of Common Criteria.

12 ISACA is an international professional association focused on IT Governance. Previously known as the Information Systems Audit and Control Association

13 SABSA Sherwood Applied Business Security Architecture

14 COBIT Control Objectives for Information and related Technology

15 DEMO Design & Engineering Methodology for Organizations,

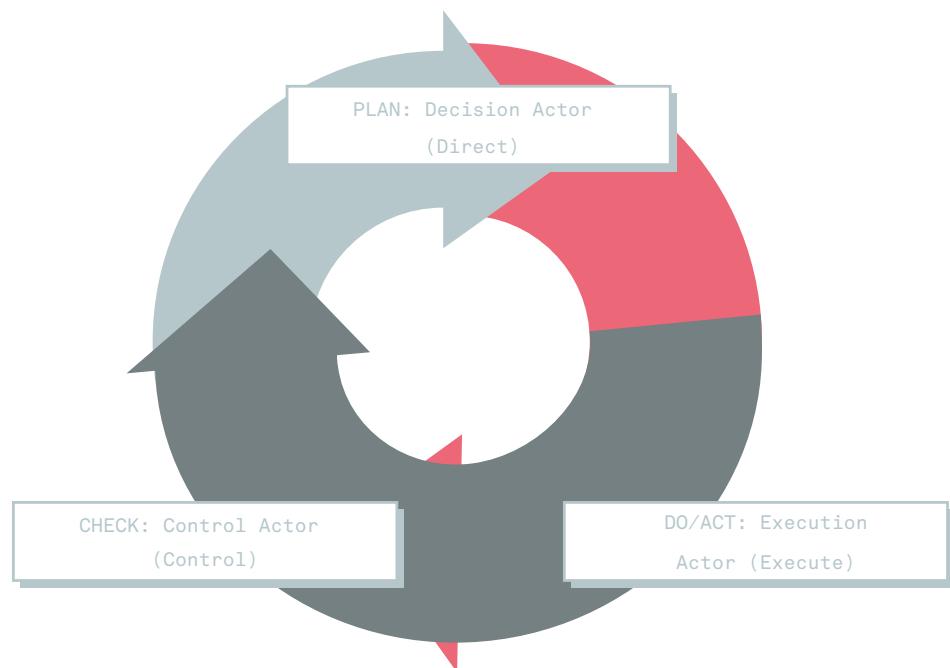


Figure 22: The PDCA cycle on Direct Control Cycle of Von Solms & Von Solms based on Tewarie [66]

in selecting and applying the appropriate model, depending on the situation or the subject to be examined. The steps needed in order to achieve the desired state of maturity are framed as **Interventions**. Interventions can be denoted as 'planning' interventions, 'doing' interventions, 'checking' interventions and 'acting' interventions (PDCA):

- Planning interventions (**Plan**) have the characteristics of formulating plans to establish objectives and processes that are necessary to deliver results in accordance with expected output. This planning requires alignment with all stakeholders involved.
- Doing interventions (**Do**) are concerned with the execution of interventions articulated in the plan. A major component of this phase is implementing controls and/or collecting factual data (evidence) in order to measure and monitor, to provide input for the 'check' and the 'act' phase.
- Controlling interventions in order to check if a certain intervention is executed to establish the desired state (**Check**). This phase requires actual and factual data collected in the previous phase in order to ascertain deviations and examine the appropriateness and completeness of the plan to enable execution.
- Interventions that are corrective in nature (**Act**). In the previous phase it is checked whether the steps taken, which are distilled from the plan, reveal an improvement according to the prior standard (baseline) or require additional corrective interventions

in order to achieve the desired state. If the CHECK shows that the PLAN that was implemented in DO is not an improvement, then the existing standard (baseline) will remain in place and require some additional learning through repeated PDCA cycles.

Tewarie mapped in his SIVA [66] research work the Von Solms and Von Solms [71] Direct and Control model as defined in 2006 [71] onto the PDCA cycle. The planning activities are carried out at the strategic level, the execution is the responsibility of management and operations, and the controlling activities are assigned to the actor who needs to check the object on quality based on compliance regulations. Tewarie made this mapping in order to reveal the relationships between the actors involved and their assigned responsibilities. Continuous improvement, as part of Total Quality Management [189], is established by executing this PDCA cycle numerous times and studying interventions, in order to understand their effectiveness during the maturing process. Edward Deming [65]¹⁶ refers to this learning element as the PDSA cycle, a Plan-Do-Study-Act [69] cycle, which builds deductive and inductive learning into learning and improvement cycles [190]. Most of the maturity models and frameworks developed within the security arena have PDCA elements incorporated.

This PDCA cycle within IS is usually designed, maintained and reported via spreadsheets [191]. Volchkov stated that collecting evidence on the effectiveness of controls in this way has limitations [72]. Filling in spreadsheets with answers to questionnaires is subject to manipulation because it is not a closed cycle. Spreadsheet data is limited to subjective opinions and leaves little room for reflection and learning, indirectly hindering continuous improvement. What's more, spreadsheet data cannot always be gathered from the original sources, which limits the authenticity, integrity and therefore the reliability of the information. Thus, Governance Risk and Compliance (GRC) tools, which were designed for large enterprises in response to the US Sarbanes-Oxley Act, were transferred from financial risk to information risk. GRC implementations are complex and the maintenance requires dedicated staff [192]. Integration of GRC tools with operational data for example via Security Information and Event Management (SIEM) is only feasible for companies that can afford expensive tooling or have sufficient staff to implement and support these functionalities [192].

3.1.4 STRATEGIC PLANNING

In literature the solution to solving Information Security (IS) issues lies in strategic planning, in directing and controlling [56]. But what are the key differences? Strategy is a method or plan chosen to bring about a desired future, such as achieving a goal or solving a problem. In the perspective of this research project strategic planning is *not* strategic thinking. Confusing these two can be misleading in the execution of a strategic plan. Strategic thinking about the desired outcome must be done by the Board. Executing (planning, monitoring, evaluating)

¹⁶ This traditional PDCA cycle was established by Edward Deming. Deming is considered the founding father of modern quality control and he strives for continuous improvement. [65]

the strategic plan to achieve these goals is the role of executive management [57], [56]. This confusion lies at the heart of the issue: i.e. most successful strategies are visions, not plans. Mintzberg states: "*When companies understand the difference between planning and strategic thinking, they can get back to what the strategy making process should be: capturing what a manager learns from all his sources and then synthesising that learning into a vision of the direction that the business should pursue*" [193]. Practising Information Security as a strategic topic has been addressed by Von Solms and Von Solms. They emphasise the leadership role that boards need to take to articulate security visions [194]. Sveen et al. point out that establishing a vision based on strategic thinking requires adequate knowledge [195]. Such knowledge gives meaning to the implications of the strategic plan, in the form of time, money and resources [196]. And it indicates the interrelationships between stakeholders.

3.1.5 INFORMATION SECURITY AS A STRATEGIC UNIQUE SELLING POINT (USP)

In 2007 Harvard professors Hunter and Westerman examined companies that treated risk management as a continuous improvement process and revealed the fact that those who did were perceived to have higher value [197]. Gordon et al. [198] examined companies which are open to voluntary disclosures concerning information security and publicly accept feedback on their security investments and activities. Here, too, there was an increase in company value [199]. A similar effect was shown in Japan [50], on the effects of information security incidents on corporate values in the Japanese Stock Market. In 2011 Shackelford [200] quotes; "*over 90% of respondents to a survey by the Ponemon Institute [201] reported experiencing a cyber-attack during the last year, costing on average more than \$2 million per organisation. Such attacks have been shown to negatively impact the stock prices of targeted firms* [200], Gordon et al. and Shackelford warn investors to be careful with investing in firms that do not proactively treat security risks. Shackelford quotes; "*As losses mount, investors will likely stop treating cyber-attacks as a corporate nuisance. Instead, they may start treating such attacks as the serious threat they are to the survival of firms and, at a macro level, the long-term competitiveness of knowledge economies built on intellectual property.*" For some companies BIS is perceived as a competitive advantage which helps them distinguish themselves from competitors [202]. Herath et al. developed a cyber-insurance model for insurance premiums using a numerical example with ICSA¹⁷ data [203]. Based on numerous publications on cyber security insurance from researchers [204], [200] and institutions [205], insurance companies such as Interpolis, AON and Chubb have been able to enter new markets with new products (cyber insurances) while others have added information security as a unique selling point in their marketing. Igor Ansoff refers in his matrix to product development and diversification of strategic portfolio planning in order to achieve competitive advantage [206]. In 2015 Ponemon and Accenture suggest in their research publication *The Cyber Security Leap: From Laggard to Leader* [165] that companies that address BIS as a strategic topic perform better and can 'leapfrog' others.

17 ICSA Labs (International Computer Security Association), ICSA Labs is providing resources for research, intelligence, certification and testing of products (source: wikipedia)

3.1.6 GOVERNANCE OF BUSINESS INFORMATION SECURITY

There are various ways in which organisations can attain their strategic objectives. Three dimensions are of strategic importance in this respect: Governance, management and operations. In this section we define Governance as "*the guidance of a setting in which others can manage effectively*", Management as "*the making of operating decisions*" [207] and the actual operations as systems in which people and processes produce products and services. These three dimensions need to be harmonised in order to achieve business objectives, aligned with the appropriate risk. Recent ISACA (Information Systems Audit and Control Association) papers on COBIT5 [208] separate Governance from Management. They are viewed as two disciplines encompassing different activities, organisational structures and therefore serving different purposes. In COBIT5, Governance is defined as follows: "*Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options, setting direction through prioritisation and decision-making, and monitoring performance, compliance, and progress against plans.*" In most enterprises, Governance is the responsibility of the Board of Directors under the leadership of the chairperson. In COBIT5, Management is defined as the discipline that "*plans, builds, runs and monitors activities in alignment with the direction set by the Governance body to achieve the enterprise objectives*" [56]. In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.

Basie and Rossow Von Solms [52] are among the few academics who have researched the area of Information Security Governance (ISG). In their study they emphasise that Security Governance ought to be part of Corporate Governance and IT Governance (illustrated in Figure 23). Their Information Security Governance definition is: "*ISG consists of the management commitment and leadership, organisational structures, user awareness and commitment, policies, procedures, technologies and compliancy enforcements mechanisms, all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times*". The importance of information, technology, people and processes [209] has transformed Information Security (IS) from a technical responsibility into an integral part of the daily business operations called "Business Information Security". Therefore, the following definition for Business Information Security Governance is relevant here; "*Business Information Security Governance (BISG) is an integral part of Corporate Governance exercised by the Board overseeing the definition and implementation of processes, structures and relational mechanisms in the organisation that enables confidentiality, integrity and availability (CIA) of the business operations towards all stakeholders*".

The word integral in this definition refers to the fact that BISG involves numerous disciplines besides IT, e.g. high-level accountability on a legal level [52]. 'Exercised by the board' implies that the highest level of the organisation is directed towards management and operation. With this definition I aim to incorporate all previous definitions relevant to Governance of

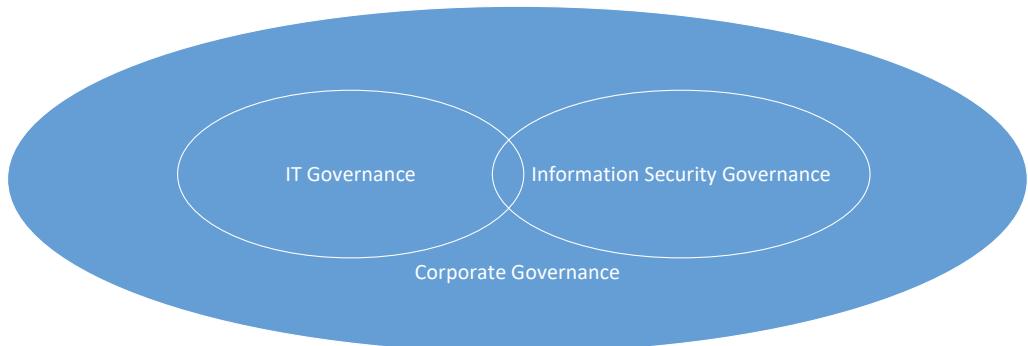


Figure 23: Information Security Governance according to Von Solms and R. Von Solms [210].

Business Information Security. Because the term 'activities' does not cover all the structures, processes and cultural aspects relevant to BIS, I use the broader terminology of "practice".

Starreveld et al. [211] defines in his theoretical model Governance, Delegation, Accountability and Control (GDAC). This model implies a continuous "Business Control Cycle" (BCC). This model is used in accountancy disciplines throughout the Netherlands. Governance relates to the highest decision actor concerned with activities such as decision-making, determining goals and ambitions (e.g. creating a mature business environment) and achieving goals. The goals are then delegated to execution actors. The agency theory [212] identifies the agency relationship where one party, the principal delegates the work to another party, the agent [59]. An example of delegation by executive management, to achieve a certain maturity ambition, could be a specific intervention or practice. The execution actor e.g. the agent, is responsible for providing "evidence-based" reporting to the accounting discipline (accountability actor). The control function refers to internal control task that act on behalf of the decision actor. The Starreveld model is used in combination with the Von Solms model in the work of Tewarie [176], which is also applied into practical environments. Tewarie distinguished Starreveld's governance model and De Leeuw's system paradigm [213] in order to differentiate activities at the governance and management levels. Activities at management level are planning, implementing and controlling the operational level. The relationship between the actors mentioned are based on the "principle-agent approach" in which two actors depend on each other, to avoid conflict of interest and establish control agreements in order to achieve mutual goals and with equal interest. In governance studies this is referred to the Stewardship theory, where directors are regarded as the stewards of the company's assets and will be predisposed to act in the best interest of the shareholders [214].

This entire governance and executive management body operates through structures, processes and relational mechanisms [215]. COBIT [56] and ISO38500¹⁸ applied these theoretical foundations to their Body of Knowledge.

RESEARCH RELEVANCE

In the light of Von Solms analysis of the beneficial effects of the exchange of practices between Corporate Governance practices and Security Governance, research into Corporate Governance practices is needed. Following the strategic organisational theory of De Wit & Meyer [216], De Haes and Van Grembergen researched "effective" IT governance practices and their ease of implementation [217]. Their Governance practices have been successfully applied into organisations and are therefore also relevant to the aim of this research.

3.1.7 INTERVENTIONS & PRACTICES

An intervention is an activity or event that changes the current status quo into a desired state, i.e. it involves the development of the organisation. In relation to the maturing process of Information Security within the organisation this requires insight into a current situation, maturity models that relate to this view, and insights into the activities and events an organisation needs to attend in order to achieve the desired state. Cummings and Worley [218] define the term **intervention** as "*a sequence of activities, actions, and events intended to help an organisation improve its performance and effectiveness*". In order to establish a desired outcome the authors emphasise the importance of intervention "design principles". "*Intervention design, or action planning, derives from careful diagnosis and is meant to resolve specific problems and to improve particular areas of organisational functioning identified in the diagnosis*". In order to distinguish effective interventions that are relevant for the influence and measurement of Business and IT Alignment (BITA) Pols [123] adopted the Cummings and Worley method in order to establish a core set of interventions that contribute to influencing and measuring BITA. These interventions have been applied in consultancy practices throughout the Netherlands.

Therefore, in this research project, we also adopt the Cummings and Worley design principles for interventions such as situational factors that must be considered when designing any intervention [219]. In this research we refer to the following more precisely formulated situational factors: Barriers, Practices, Critical Success Factors and Preconditions that enable or limit organisational development (OD). The authors also refer to readiness for change. This element is addressed in this research due to the use of numerous methods to engage all relevant stakeholders (i.e. mid-market companies, security professionals, experts, target groups) [220], [221]. The capability to change is addressed through the element "resource capabilities", which denotes the elements that are required in order to determine capability (skills, experiences, competences, knowledge) and ability (willingness, commitment, culture) [222]. By engaging the environment (organisations) in this research

¹⁸ ISO/IEC 38500 is the international standard for corporate governance of information technology (IT).

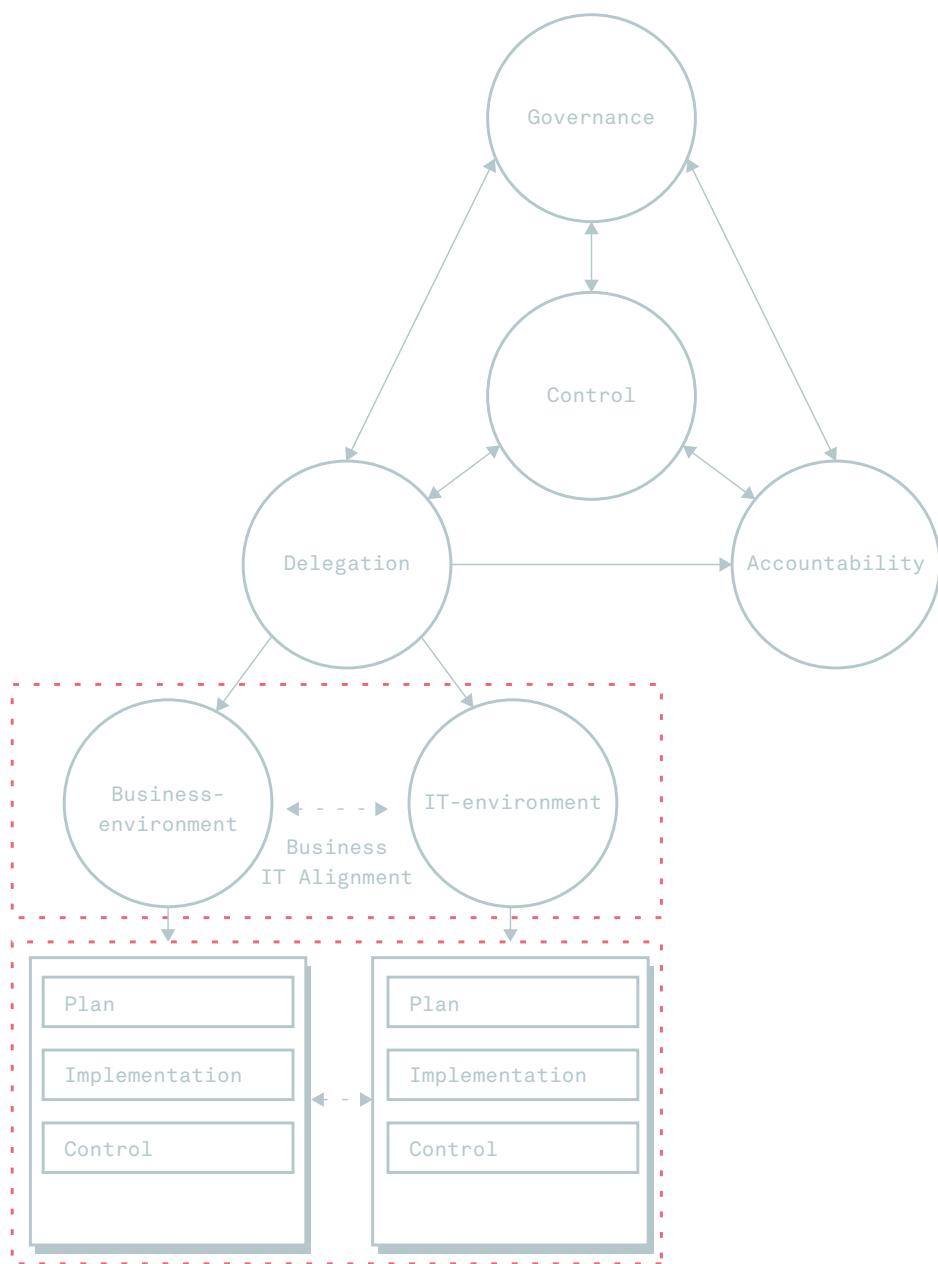


Figure 24: The conceptual model of GDAC processes based on Starreveld et al. [211] & De Leeuw [213].

project the Capabilities of the Change Agent are addressed, hence the fact that; “*Many failures in OD result when change agents apply interventions beyond their competence*”. An interesting finding from Pol’s research is that most of the derived interventions are indeed general Business Management practices (page 439). An interesting research assumption in relation to BIS is if the *interventions and practices that can be applied to BIS in fact originate in generic business management principles*.

PRACTICE

In the context of this research project we refer to practices as a working method or activity introduced to establish or maintain a certain state. A collective set of practices can be part of a larger whole, e.g. an intervention. In this research project we relate to interventions as a set or sequence of activities, working methods or practices with the objective to help an organisation improve BIS maturity. A security control such as identity and access management is considered a control and is part of one or more activities. As mentioned above, a situational factor can be a practice that is applied prior to the execution of the intervention in order to increase its effect [218].

3.1.8 STRUCTURES, PROCESSES AND RELATIONAL MECHANISMS

Strategic management theories address the core purpose of the company and the desired organisational design needed to achieve business goals. These methods capture all of the dimensions that could influence the desired outcome. In the book *Strategy Synthesis*, De Wit and Meyer [223] advance a strategic organisational theory, containing three major components of an organisation: Firstly, *Organisational Structures* (the firm's anatomy), for instance the hierarchical reporting lines within a firm or towards regulators or other stakeholders. Secondly, *Organisational Processes* (the firm's physiology) i.e. processes and procedures for the most efficient organisation of a firm: escalation and communication processes; knowledge and competences processes. Finally, they distinguished *Organisational Culture* (the psychology of the organisation) e.g. awareness, participation and collaboration. In this research we use the more exhaustive terminology *Relational Mechanisms* (RM) because it addresses additional soft and intangible factors of an organisation such as perceptions, attitudes, behaviour, leadership, etc.

This SPRM theory, which was successfully applied in several previous studies [105], [111], led to an effective framework for the Enterprise Governance of IT. Due to the research work of Steven De Haes at Antwerp Management School and his involvement in the COBIT5 for Information Security review process, ISACA adopted the integration of SPRM into the COBIT5 model [56]. Hence this management model, which was based on work by De Wit and Meyer, is being successfully applied by boards to enable better dialogue with upper management. This theory-based business approach also shows its practical contribution [187] to the financial sector environment in Belgium as well as Bodies of Knowledge such as ISACA’s COBIT5 for Information Security [56]. Hence this De Wit and Meyer theory,

which enables a decomposition of the strategic elements, increases the awareness of upper management and categorises the numerous interventions and practices to be explored, is therefore considered in this research project.

3.1.9 REQUIREMENTS

There are several forms of requirements. According to the Business International Institute of Business Analysis in their Guide to the Business Analysis Body of Knowledge (BABOK) a classification of several requirements is made. Three major ones are:

- *Business requirements* relate to the overall statements of the business goals, objectives, or needs of an organisation.
- *Architectural requirements* relate to the explanation of identifying the necessary systems structure and systems behaviour.
- *User (stakeholder) requirements* relate to mid-level statements of the needs or demand of a particular stakeholder (regulators, customers, civilians) or group of stakeholders. They usually describe how someone wants to interact with the intended solution. Often acting as a mid-point between the high-level business requirements and more detailed solution requirements¹⁹.

According to Wieringa [224], "A requirements specification consists of a specification of product objectives and a specification of required product behavior". "The generic objective of any product is to answer needs that exist in its environment. Any development process starts with a statement of product objectives and produces behaviour specifications and product decompositions along the way". Wieringa defines business needs as the initial starting point for setting requirements. The needs, for example business problems, are translated into product objectives which are defined in terms of the product and specifications about desired behaviour of the product. Each product specification is a statement of objectives for its subsystems. In client-oriented development, "the needs of the client may even change because of the determination of objectives. This is called requirements uncertainty. The characteristic feature of product evolution is that an evaluation of experience of the product after it is developed, leads to a (re)development of the product. The logical structure of product evolution is the same as the logical structure of feedback control" [224]. We call the initial process of defining functional and non-functional technical requirements in the first iteration of the artefact an 'experiment'. It is not necessary to be completely precise and exhaustive when exploring these requirements. The initial aim is to work on establishing initial requirements that cover most of the problem. The objective is to engineer an artefact that can serve numerous stakeholder needs and – due to its experimental stage – accept uncertainty and 'fuzziness' during development [225]. In later iterations of the artefact, additional requirements can be built in, based on reflections and feedback from the user community. According to Wieringa in client-oriented development, "the needs of the client may even

19 Source: A Guide to the Business Analysis Body of Knowledge (BABOK) Guide version 3

change because of the determination of objectives. This is called requirements uncertainty. The characteristic feature of product evolution is that an evaluation of experience of the product after it is developed, leads to a (re)development of the product. The logical structure of product evolution is the same as the logical structure of feedback control" [224]. Thus, in this thesis practical problems and business issues items relate to "business requirements". These items require something from the business in order to bring about the desired outcome or solve a particular problem. This can be achieved by articulating and implementing certain functional or non-functional requirements in an artefact.

INFORMATION RISK AND SECURITY REQUIREMENTS

Wieringa [226], wrote numerous publications on setting requirements for software security, according to Ionita, Bullee and Wieringa "*Information Security Risk Assessment can be viewed as part of requirements engineering because it is used to translate security goals into security requirements, where security requirements are the desired system properties that mitigate threats to security goals*". In order to automate the secure software development process based on risk analysis, Yu et al. [227] proposed an automated analysis of security requirements through risk-based argumentation via RISA. RISA (Risk assessment in Security Argumentation), "*uses public catalogues of security expertise to support the risk assessment, and to guide the security argumentation in identifying rebuttals and mitigations for security requirements satisfaction.*" [228] The empirical validation made by Yu et al. included proposing a product called OpenRISA, which contributes to solving three major software security problems. The following are important considerations for this research project:

1. Vulnerabilities – due to the lack of secure software modelling and development – are integrated into the modelling language.

This 'security by design' principle is applied in this research since it embodies continuous learning and improvement via feedback and feed-forward loops, in close collaboration with stakeholders (in order to ensure safe products and processes (e.g. artefacts)) [70].

2. The lack of a continuous feed of software security improvements from the existing body of knowledge is resolved via automated feeds of publicly available libraries.
Existing frameworks are used in this research in order to develop, maintain and utilise security best practices.
3. The lack of formalised arguments; these are challenged and checked for soundness in prior security risk assessments. This rigorous method contributes to more robust software design and development.

Open collaborative dialogues are used to reflect, learn and prioritise, thus enhancing existing bodies of knowledge. Empirical testing is used to achieve improvements in the practical environment.

3.2 CONCLUSION

In this chapter we have identified and defined the concepts that relate to the research questions set in chapter 1. It is not the objective to be exhaustive with all concepts. It is the primary aim to demonstrate correlations and viewpoints from various sources how BIS is perceived and practiced. It provides guidance for the further research and reader to appreciate research deliverable 1. *A, the conceptual framework for BIS.* Out of this chapter we can derive a definition for BIS maturity; BIS Maturity is the state, process or period of being mature as an organisation when it comes to Business Information Security, expressed via a maturity model which constitutes of multiple levels with predefined criteria. With Business Information Security we address the entire End-to-End process of information processing including all relevant stakeholders.

4

EXPLORING MANAGEMENT INTERVENTIONS FOR IMPROVING THE Maturity OF BUSINESS INFOR- MATION SECURITY

4.1 INTRODUCTION

In this chapter we examine the results of an exploratory study that uses literature study, expert panel research via GSS and survey research to examine contributing interventions to the process of maturing the level of Business Information Security (BIS). First we define, based on literature research, some key concepts and second we examine the results of the study. The research also examines barriers for not implementing these interventions by the organisations. This chapter finalises with proposing a minimum core set of interventions for organisations as well as new insights and requirement propositions for the measurement of BIS via Design Science Research Artefact construction. It describes the Design Science Research process of researching the literature (Rigour Cycle) on interventions and practices, scrutinise the latter via a GSS expert panel research and present them as requirements for the first iteration of the artefact (Design Cycle) in Chapter 6. To later on be validated in practice (Relevance Cycle) in Chapter 7.

This chapter was partly published in the International Journal of IT/Business Alignment and Governance (IJITBAG) 1(4), Page 18-39, in December 2010 under the title *A research journey into Maturing the Business Information Security of Mid-market organisations*.

4.2 DEFINING THE MID-MARKET AS A RESEARCH AREA

A segmentation of the market in order to carry out research has been made by Gartner. Gartner defines small and mid-sized business (SMBs) "by the number of employees and annual revenue they have. The attribute used most often is number of employees:

- *small businesses are usually defined as organisations with fewer than 100 employees.*
- *mid-sized enterprises are organisations with 100 to 999 employees.*

The second most popular attribute used to define the SMB market is annual revenue:

- *small businesses are usually defined as organisations with less than \$50 million in annual revenue*
- *mid-sized enterprises are defined as organisations that make more than \$50 million, but less than \$1 billion in annual revenue [229].*

Gartners' main focus is on the United States. To examine the European and more specifically the Dutch market, a definition of this market made by the Central Bureau of Statistics in the Netherlands (CBS) is used. CBS defines medium-sized organisations – also known as mid-market organisations – as those providing work for 50-100 employees. In the appendix a list of selected branches, with numbers of employees defined according to several sources is added. As the European Commission increasingly emphasises the importance of information technology, this research partially follows this EU definition of mid-market segmentation criteria. Partially, because when considering the number of employees, the European

Commission defines the limit of mid-market organisations as 250 employees.

ENTERPRISE CATEGORY	HEADCOUNT	TURNOVER	OR	BALANCE SHEET TOTAL IN €
MEDIUM-SIZED / MID-MARKET	< 250	≤ € 50 million		≤ € 43 million
SMALL	< 50	≤ € 10 million		≤ € 10 million
MICRO	< 10	≤ € 2 million		≤ € 2 million

Table 2: Market segmentation according to the EU Commission based on headcount and financial figures.

An important observation is that 250 employees do not equal the number of automated systems (servers, PCs, printers) a company is using. In theory a potential security breach can be caused by an 'actor' (i.e. a person, system or application) that is directly or indirectly connected to the internet, creating some form of a threat. Such threats will increase as more and more managed corporate devices are connected to the internet, not to mention non-managed corporate devices and Internet of Things (IoT) devices. According to Deloittes' report on mobile usage in 2013 a Dutch individual has 4.3 devices at his or her disposal compared to 7.3 in Spain [230] and these are seldom managed by the organisation itself. They create a form of Shadow IT that poses an increasing risk to organisations [231]. This is why it is hard to determine the exact number of systems. In practice a company defined as a mid-market organisation, with 250 employees, for example a factory, can have 10 systems to run their business. Based on the EU criteria²⁰ this factory would be in the mid-market, but from a research perspective it is small.

Another method used to measure the size of a business, and to define mid-market segmentation, according to the European Commission, is the annual turnover or the balance sheet total. When companies exceed a total amount of annual revenue or have a certain balance sheet total, they do need to comply with certain reporting regulations, for example IT audit regulations and "wet op de jaarrekening" [232]. Taking into consideration the limitations of employee headcount and the limitations on disclosure, I define the mid-market segment based on automated systems. This way of counting and selecting organisations is fairly effective and plausible with respect to the research problem. On the one hand, the number of systems tells us something about the reliability on IT for the business processes, and thus the potential IT risk profile. And it tells us something about the type of industry the company is in (generally factories have fewer systems than, for example, banks) and, on the other hand, the estimated revenue. This provides an indicator for the relevant legislation that might be applicable. We cap the number at 2500 systems. Generally, organisations with a higher number of systems have security management practices in place.

20 Taken from the European Union website: <http://eur-lex.europa.eu/>

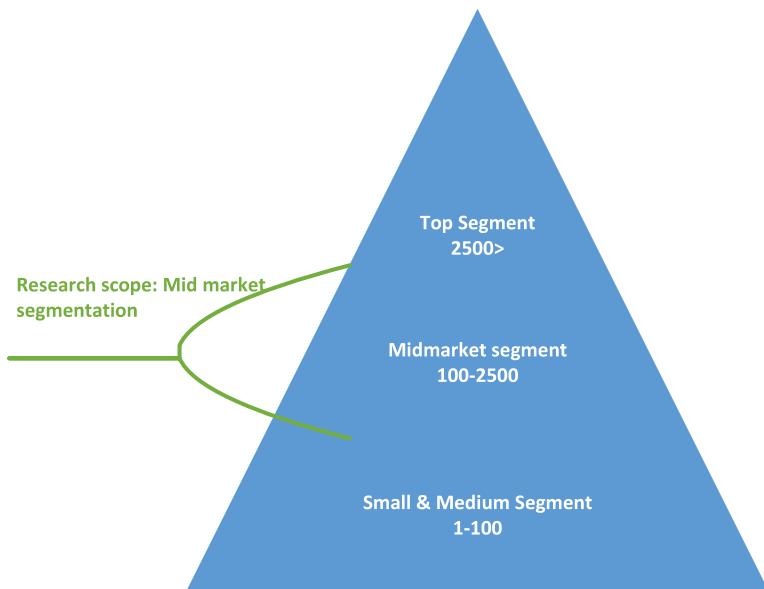


Figure 25: Market segmentation based on number of systems.

4.3 PROBLEMS FOR MID-MARKET ORGANISATIONS

In chapter 1 the main problems organisations face nowadays are described. It seems hard to cope with rapidly changing threats on one hand and upcoming business demands on the other [209]. Enterprise focused frameworks to operationalise the IT, in order to align with the business goals, seem to fail mid-market companies [87]. This mid-market segment, with 100-2500 systems, is increasingly subject to cyber threats [233], [234] and the lack sufficient knowledge [235] about attainable interventions in order to become security compliant [87]. The problem of insufficient knowledge about security interventions in this segment and the increase in security incidents subsequently led to the research questions described in chapter 1 to examine which interventions mid markets can adopt in order to increase the BIS maturity. Summarized in the question; *What set of interventions, based on a best-practice maturity model, can be applied to enhance the maturity level of business security within mid-market organisations?*

Various studies [236], [237] present many interventions that contribute to an increase of the security maturity levels of an organisation. However interventions that are essential and which are actually effective and easy to implement for mid-market organisations have not yet been studied. This led to a scientific approach of selecting, comparing, validating and presenting

effective and easy to implement interventions that increase business information security, i.e. a core set of interventions. The data for this research was collected during the first two quarters of 2010 in the Netherlands.

4.4 RESEARCH APPROACH FOR EXPLORING MANAGEMENT INTERVENTIONS

The main objective of this research project is to select, assess and present effective and easy to implement interventions that increase business information security, i.e. a core set of interventions. The research method we use in this part as described in chapter 2 is; literature research to explicate the problem, GSS for judgement and prioritisation of interventions and finally Delphi research to validate the practical management interventions gained earlier via GSS. These selected interventions derived from experts with GSS are presented to the market in order to achieve "real-life" validation on applicability and acceptance of these interventions. This approach is visualised in Figure 26, the conceptual model of this research. Also potential barriers that might hinder the implementation of these interventions were investigated.

To investigate which interventions are required as a core minimum several steps are taken in order to collect answers to the research questions. These questions directly relate to the research questions set forward in chapter 1:

1. *What is BIS maturity, based on the definitions derived from best practices and the literature?*
2. *Which best-practice interventions are currently used to improve BIS maturity?*
3. *Which barriers do organisations experience when applying BIS interventions?*
4. *Which barriers have been identified in mid-market organisations?*
5. *Which of the identified BIS interventions are practical in such organisations?*
6. *What are the general organisational preconditions for the application of the core set of BIS interventions?*

To provide answers to these research questions, relevant literature on maturity models and interventions, which interventions exist and which best practice can be applied, was performed. In order to prioritise interventions for mid-markets it is essential to select interventions that are required by law and which are effective and easy to implement, according to academics and practitioners. All selected interventions were assessed by experts' via an expert panel interview. These experts carefully assessed all relevant interventions based on 'ease of implementation and effectiveness' ranked on a scale ranging from -5 representing not contributing, 0 being neutral and +5 being very contributing. In addition the experts were asked to list barriers which make it difficult if not impossible for the market to implement certain interventions.

The outcome of this initial research phase was then analysed, interpreted on relevance and applicability for further research and then presented in a survey questionnaire. This survey was then sent out to 40 organisations in the mid-market segment. The survey objective was:

- to test awareness of information security law and legislation in the market
- to test the perception of current security maturity levels and required ambition levels in the coming 2 years
- to test which of the core interventions, derived from experts, are enforced within the market
- to test which barriers they experience while implementing security
- to test what they find to be the most contributing interventions in order to increase their security maturity.

The combination of expert panel research and the mid-market survey was performed in order to get answers to all the research questions but also to measure the current state of business information security of Dutch organisations and examine the initial state of maturity for mid-market organisations in the Netherlands.

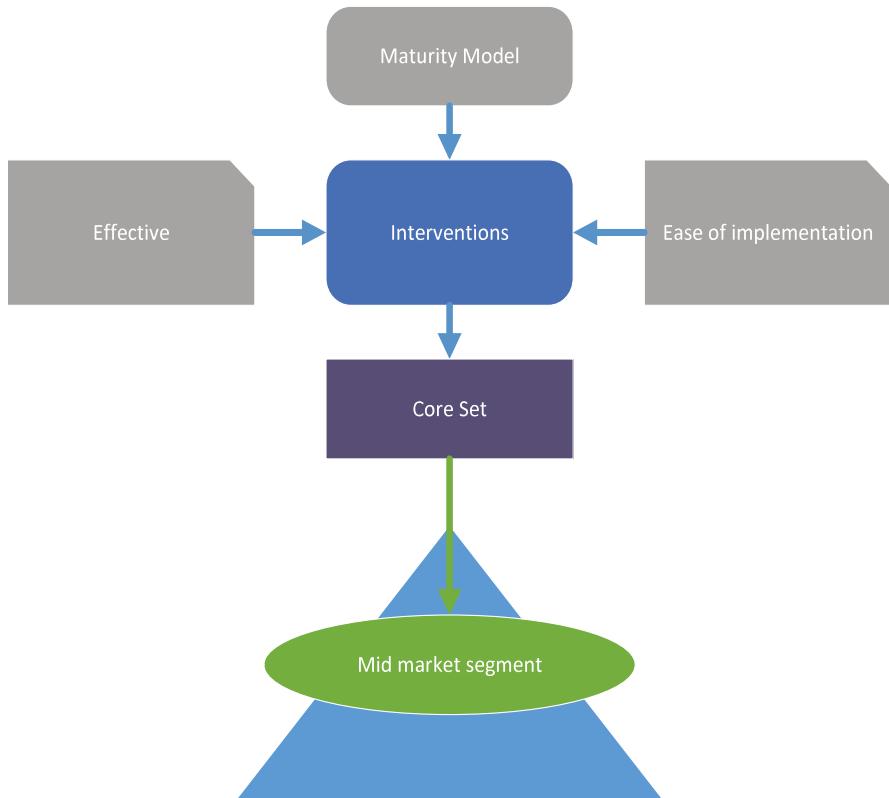


Figure 26: Conceptual model on mid-market interventions research.

4.4.1 CONSIDERATIONS FOR THE SELECTION OF INTERVENTIONS

An intervention refers to a mixture of various actions, processes or mechanisms which contribute to the security process. The following intervention frameworks were used, as source of inspiration, in order to derive the relevant interventions.

ISO/IEC 27001

The ISO (International Organization for Standardization) and the IEC (International Electro Technical Commission) have established a joint committee, ISO/IEC JTC 1, in order to deal with their mutual interest in the area of information technology. This committee has a number of subcommittees with different responsibilities. The committee responsible for information security standards and practices is the SC27. The most recent one in this range is the ISO27001 which specifies Information Security Management System (ISMS) standards. This system is designed for all organisations in every sector. It is a management system and not a technology specification. It is the first of a series of international information security standards which are all in the 27000 range [94]. The ISO27000 range has a strong relation with the other ISO standards, for example Quality Management (ISO9000), Business Continuity Management (BS25999), IT Service Management (ISO20000) and others. The ISO/IEC27001 ISMS standard adopts the Plan, Do, Check, Act (PDCA) process approach. This PDCA approach encourages continuous improvement, since information security is a complex and dynamic matter this PDCA approach is a prerequisite for good ISMS [238]. The precursor of the ISO Security standard, the British Standard (BS7799), and ISO27001 are both examples of standards that offer guidance on how to approach information security through means that have been proven to work in many organisations [239]

ISO/IEC 27002

The objective of the ISO/IEC 27002 is to provide information to organisations responsible for implementing information security [94]. It is a best practice for developing and maintaining security standards and management practices within organisations to improve reliability on information security in extended enterprise relationships. It specifies 138 security controls in 11 domains. It emphasises the importance of risk management and elaborates that it is not mandatory to implement every control in each domain (only those controls that are relevant). The controls vary in the domain of: security policy, organisational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management and compliancy.

The combination of the ISO 27001 and 27002 standard provides a useful model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System. ISO provides a clear description of a security policy and implementation of its interventions [175]. In this research we use the ISO27002

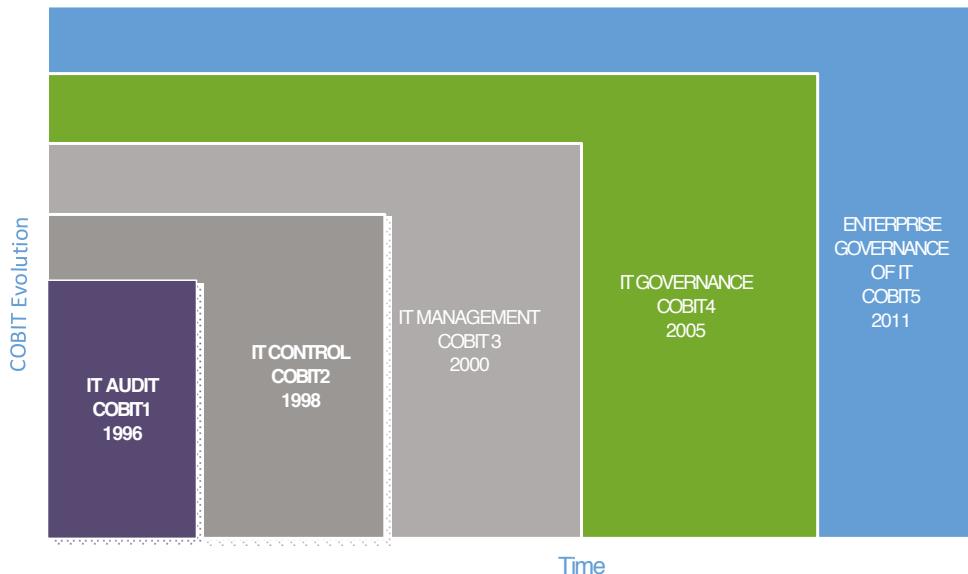


Figure 27: Evolution of COBIT.

controls (version 2005) as a source of potential core interventions that is going to be examined by experts on numerous perspectives.

COBIT

Control Objectives for Information and related Technology (COBIT) has been an internationally accepted set of guidance materials for IT governance since 1992. It is developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) [240]. The aim of COBIT is to translate business objectives to IT Goals to IT processes to assist in the actual implementation of effective IT governance throughout an enterprise. In December 2005 version 4 was introduced. In version 4.0 the overlap with the ITIL framework was reduced and the alignment with ITIL practices improved, which led to a direct relation to the business objectives [237]. Several information security controls (according to the Code of Practice) were introduced in the COBIT framework. In December 2007 COBIT4.1 was developed which was mainly driven by studies performed by the University of Antwerp Management School [108], [105]. COBIT currently receives more attention because the current version 5 is more suitable and better applicable to compliance requirements. This version helps organisations to operationalise their IT in such a way that they are compliant with regulations such as Sarbanes-Oxley (SOX), Committee of Sponsoring Organizations of the Treadway Commission (COSO), Basel III and PCI DSS for payment card industries.

COBIT is appreciated for its enterprise wide perspective and integration with project management standards such as PMBOK, Prince2 and architecture frameworks such as TOGAF. The COBIT version 4.1 is updated as a result of the University of Antwerp Management School studies and COBIT users input [108]. This resulted in the COBIT5 for Information Security [56]. It is more pragmatic in nature now and therefore more suited to adoption by the mid-market segment. The perception of the complexity of COBIT is reduced with version 5. Important changes that contribute to the 'acceptance' of COBIT by mid-market organisations are:

- Enhanced executive overview and clear directives [209];
- Improvement of the list of business goals and IT goals as a result of Antwerp Management School studies [241], [187], [105], [109], [215];
- Explanation of goals and metrics in the framework section [217];
- Better definitions of the core concepts. It is important to mention that the definition of a control objective changed, shifting more towards a management practice statement;
- Improved control objectives as a result of updated control practices and Val IT²¹ activities;
- Application controls have been reworked to be more effective, based on work to support controls effectiveness assessment and reporting.

In order to successfully execute the business objectives, for example to be compliant with regulation, an IT organisation can effectively use the facilitating function of IT. The COBIT framework contributes to this by making a direct link from business objectives to organisational –security- controls. The improvements for version 5 are based on the view of enterprise governance defined by ISACA's Taking Governance Forward (TGF) initiative. The COBIT 5 Process model reflects the main topics and demonstrates the incorporation of industry best practices. Relevant industry standards and best practices are mapped on COBIT5 in the appendix of the COBIT5 for Information Security. The most relevant ones are mentioned below (taken from COBIT5 for Information Security, page 59 [56]):

- The 2011 Standard of Good Practice for Information Security, Information Security Forum (**ISF**), UK, 2011
- **ISO/IEC 27000** series
- National Institute of Standards and Technology (**NIST**)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (**OCTAVE**), Carnegie Mellon Software Engineering Institute (SEI)
- Payment Card Industry Data Security Standards (**PCI DSS**)
- The Business Model for Information Security (**BMIS**) [209]
- Common Security Framework (**CSF**), Health Information Trust Alliance (**HITRUST**), USA, 2009

²¹ Val IT is a governance framework (based on COBIT) that consists of a set of guiding principles, and a number of processes conforming to those principles that are further defined as a set of key management practices (www.isaca.org).

- Health Insurance Portability and Accountability Act (**HIPAA**)/Health Information Technology for Economic and Clinical Health (**HITECH**), USA, 1996 and 2009, respectively

With respect to this research and its objective, to get the top interventions and their framework accepted by the mid-market, I would like to emphasise the following main considerations for the mid-market:

1. Since, businesses are more web-centric, focused risks related to information are increasing. In order to keep up with information security risks that might impact the business continuity it requires more Business and IT alignment. COBIT enables business and IT alignment and because it also incorporated security management it also enables business and security alignment;
2. Business executives require understanding and control of IT-related investments throughout the lifecycle [242]. COBIT provides a proven method to assess whether IT services and new initiatives are meeting with business requirements and are likely to deliver the benefits expected;
3. This mid-market segment requires standardisation, preferably by an international accepted standard [4]. COBIT is a widely adapted and accepted international standard. And ISACA has a proven community and track record throughout the world. It provides an authoritative, international set of generally accepted practices that helps boards of directors, executives and managers increase the value of IT and reduce related risks;
4. This mid-market segment requires an out-of-the-box framework of principles and controls to contribute to policy development [233]. COBIT provides guidance in principles and controls to initiate and maintain a clear policy. The minimum standards provided by other bodies such as NIST, ISF can be integrated in the COBIT framework, or left our if desired [237];
5. This mid-market segment requires a clear insight in investments on IT and security [62]. COBIT provides directions to ensure that (IT) investments support the business. It relies on respected project management practices such as Prince2 and PMBOK;
6. If stricter EU regulations require an IT Governance framework COBIT is likely to be the one, due to its proven track record and wide acceptance by enterprises and financial institutions [60] [91];
7. From a business security perspective, measure, monitor and act (PDCA) are at the core of the mitigation of risks. This mid-market segment requires a framework that enforces that principle. It requires insights into its security maturity level in order to take necessary steps to the desired ambition level. Because of the adoption of ISO's ISMS and a Maturity Model this segment can benefit directly. COBITs' maturity model taken from 4.1 or the ISO15504 maturity reference models can be applied in the overall framework.

The application of capability and maturity models enables more efficient and successful auditing and benchmarking (Sox audits, DNB Audits [91]; GBA audits²², EDP audits, NEN audits or ISO audits). In this research it is the objective to explore a core set of Information Security interventions that contribute to measuring, monitoring and thus improve the maturity level of the organisation. Thus the objective is to examine interventions and not the effect of the applicability of individual standards or frameworks such as ISO2700X. The ISO27000 is used as repository to examine the intervention candidates through the use of experts and mid-market organisation validation.

4.4.2 SELECTING THE SOURCE OF INTERVENTION CANDIDATES

To achieve acceptance in the target market segment, a widely adopted standard is desired [87], referring to a holistic approach to information security that addresses people, processes, legislation, and IT aspects [238]. For the qualitative collection of the data, a combination of qualitative research and quantitative research is performed. The initial step was to select a framework or norms that encompass intervention candidates that might be relevant for mid-markets. To collect this data numerous sources with technical controls, process controls were reviewed and compared due to the current literature on framework and control mapping [237]. The selection of candidate interventions is subject to several perspectives that needed to be considered. These perspectives are based on the "*Ten Deadly Sins of Information Security Management*" which was published in 2004 by Von Solms and Von Solms [194]. The authors list numerous dimensions that require attention when successfully adopting Information Security.

COMPLIANCE PERSPECTIVE

First, compliance regulations form an important incentive for increasing business information security maturity, as these organisations simply must comply with certain minimum standards. For example, in the Netherlands medical organisations need to be compliant to the NEN which is mainly based on the ISO27K standards. Government organisations need to be compliant to the Baseline Information Security Government (Baseline Informatie beveiliging Rijksdiensten). In the preselection, we consider interventions and frameworks that are known, approved and prescribed by the authorities and regulators.

BUSINESS PERSPECTIVE

Secondly, security is no longer an IT issue only. To align the business more with security, it required to preselect interventions that do just that. So the condition for the intervention framework was that they need to be understandable and acceptable by the business, its managers and its owners.

AUDIT PERSPECTIVE

Third, standardisation in financial reporting, to be 'in control' is another incentive why organisations *Must* increase security maturity [92]. This is valid for large and relatively smaller organisations (> € 8 million in annual revenue). In the preselection, we considered interventions that act as a standard for security and encapsulate the CIA triad of Electronic Data processing (EDP) auditing. This audit and assurance perspective makes it necessary not to define mid-markets as SME but as ME and larger, e.g. mid-market. As mentioned in the previous sections.

QUALITY PERSPECTIVE

Forth, when organisations do not need to comply but have a sense of urgency to increase security maturity from a quality perspective the interventions need to do just that. They need to promote the quality of the business information or assure its confidentiality, integrity and availability in the first line of the business. The suggested interventions preferably had to follow other quality methodologies such as Deming's Plan, Do, Check and Act or embrace quality norms such as ISO (9000). When building security into processes and technology 'by design', it reduces the chances of risks and security controls that need to be built in afterwards.

MATURITY PERSPECTIVE

Last, when organisations want to make sure where they are in the security maturity process the need to have interventions that contribute continuously. Once interventions are selected they need to be as generically as possible and exchangeable with other maturity models and have focus on "The Measurement/Metrics" [194].

These perspectives form an important source of inspiration when selecting a frame of reference that can be used when selecting MBIS intervention candidates.

4.4.3. ISO AS A FRAME OF REFERENCE FOR BIS INTERVENTIONS

FIRST SELECTION

With the above-mentioned perspectives in mind, the interventions suggested by the Code of Practice are considered to be most applicable because they are used globally and are generally accepted in the ISO 27000 range. From a compliancy perspective, the list of interventions (controls) in the ISO27002 is generally accepted. For example, when organisations need to comply with the norm, the suggested interventions in this norm are derived from the same Code of Practice. Also, to make sure that companies comply with the financial reporting norms EDP auditors use the interventions described in this ISO norm (Code of Practice). The suggested interventions also address management involvement and make sure the security policy is enforced by senior management before it can take effect in the operation (e.g. IT). Addressing the business domains as well as contextual influences such as laws, regulations (art 15) and business partner security (art 10). ISO27001

integrated their ISMS (Information Security Management System) as a process approach. Ensuring that security is seen as a continuous process rather than an end state, the Deming Cycle is introduced and incorporated into the interventions (art 13, 14). Several scientists demonstrate the successful mapping of ISO to a maturity model [175], [243], [244]. The interventions are generic and can be applicable to numerous security maturity models. The organisations' security maturity ambition determines the applicability of the intervention on a certain level. Thus ISO provides potential core interventions that can be used as a source of inspiration for this MBIS research into core interventions. The objective of this research is to distil core interventions based on the 138 controls/intervention candidates. It is *not* the objective to test the individual effect of the controls or to do qualitative research on applying the ISO2700X standard or ISO27002 controls.

2ND SELECTION OF INTERVENTIONS

A total of 138 interventions in 10 categories that cover the necessary elements, from e-commerce security to physical security, etc. From 138 interventions covering all elements, we want to establish a core minimum set that can form a frame of reference. A certain number of these interventions are generic and thus require additional selection to ensure mid-market 'relevance'. The objective is not to be exhaustive, but to be concise, with a minimum core set of essential interventions that are relevant to the mid-market segment and contribute to improving the maturity of business information security. Some of the criteria are for example generic, large enterprise-oriented and budget-intensive. thus there was a preselection of these interventions, before the experts started assessing a large number of non-relevant interventions. Siponen and Willison [3] addressed the 'suffocation effect' of having too many controls and the complexity of frameworks resulting in organisations not being effective in their information security [3], [151]. Some examples of less relevant managerial interventions for mid-markets are:

1. synchronisation of time clocks; synchronisation of the clocks is important, but only contributes indirectly to improving BIS maturity
2. management of network routers (11.4.7)
3. management of network session timeouts (11.5.6)
4. systems for password management (11.5.3).

Such interventions are necessary, but mainly in the technical domain. Thus, for this second round the objective was to preselect BIS management interventions that are relevant for mid-markets and can serve as intervention candidates to be examined by experts. A certified ISO 27000 lead auditor (CISSP, CISA, CISM²³) was asked to judge the selection of all 138 interventions. This individual acts as a trainer for ISO auditors and has more than 10 years of experience in security management and ISO audits. He or she was asked to assess each of the 138 interventions on relevance for mid-market organisations. An extra external assessor filtered the total of 138 interventions to ensure objectivity in the preselection phase. The final

23 Official Security Certifications: CISSP, Certified Information System Security Professional, CISM, Certified Information Security Manager, CISA, Certified Information Security Auditor

list of selected interventions derived in this step can be found in the appendices of Chapter 4. The total number of interventions selected by the lead auditor is 58.

MINIMUM PERSPECTIVES

Apart from the perspectives mentioned above, organisations who consider doing business (transactions) via the web, house intellectual property, pursue a spotless reputation or handle confidential information comply with a limited set of minimum basic interventions.

1. EDP AUDITING PERSPECTIVE

For mid-market organisations with more than 75 personnel and more than €8 million of annual revenue, an audit on IT systems is performed in order to insure the statement of 'in control' from the accountant. This law is compulsory for companies that are listed. Mid-market segment organisations will need to comply with this EU regulation in the years ahead. In order to select the core interventions that contribute to this demand the EDP auditing criteria were used for the selection. This exercise resulted in a set of 50 (of the 58) interventions to take into consideration from an EDP auditing perspective. Thus eight interventions were dropped due to the fact that these are not directly required for EDP audits.

2. ISO AUDITING PERSPECTIVE

For mid-market organisations that want to comply with ISO and later on want to audit themselves, another criteria is applied in this selection: the ISO auditing clauses. This preselection, also performed by the lead auditor resulted in another additional 19 candidate interventions, taken from the ISO standard, due to the fact that these are required in order to become compliant with the ISO standard. This resulted in a new set of 69 interventions (50+19).

This new set of 69 interventions derived from the ISO standard, filtered on the basis of multi-criteria from multi-perspectives are considered relevant to the mid-market segment. The qualified list of 69 interventions was not fully completed and the mid-market may, themselves, need to consider other necessary additional interventions. These final suggested interventions are a guide towards the objective of a minimum, but essential, intervention set in order to improve MBIS. The next step was to further investigate, assess and judge these 69 interventions with experts via qualitative research, named the "expert panel research". This was done via a Group Support System research method. The steps described are visualised in the diagram below.

This research phase has the intention to, based on a preselection of relevant intervention derived from a representative frame of reference, to establish via experts a core set of interventions for mid-markets. The use of experts in combination of GSS enables to brainstorm, discuss and raise additional relevant interventions that are not yet present in the BoK or have been overlooked in the initial step.

4.4.4 EXPERT PANEL RESEARCH FOR THE SELECTION OF MID-MARKET INTERVENTIONS

All previously selected interventions now need to be assessed from an expert perspective. In this research an expert is a person with the following characteristics: Extensive track record in security management as a scientist or practitioner. A Master's degree (or certified at the same level) in the field of security management and or certified by Code of Practice / ISO and or certified auditor and/or accounting auditor. An expert has more than 15 years of Information Security and Risk management experience within large enterprises. The objective of making use of experts is to collect qualitative data, argumentations and justifications on certain interventions. To have an expert view if interventions are applicable, attainable or acceptable and on the basis of which criteria. Six experts were selected to judge the latter. Hereby the size of the group does not have to negatively influence the duration of the meeting. On the contrary, larger groups can influence the quality of the meeting and decision-making process [118].

The expert session programme was divided into five parts to structure the process and aim for maximum output. The expert panel session began with a clear presentation about the expert session objectives and the background and motivations of this research project. The research problem and the research approach (i.e. how to gain certain data from various angles) were presented. At the beginning of the session, the researcher clearly stated what the expected outcome should be – a core set of interventions for the mid-market - and why a certain output was required (rank of top interventions) in order to further the research (questionnaire survey for the mid-market segment). In this way the complete group clearly knew the goals and the expected end result.

Numerous business and IT alignment studies [245], [186] have been performed by scientists including summaries of studies, best-practice interventions, similarities, etc. and others proceed on those studies. Van Grembergen and De Haes [105] have investigated "Practices in IT Governance and Business IT Alignment". They look at how mid-sized to large financial service organisations implement IT governance to achieve a better alignment between the business and IT. Their primary objective was to come up with a minimum set of practical interventions to increase the alignment between business and IT and pre-describe a core set of (expert -fed) interventions in order to Governance IT. This resulted in a practical frame of reference to implement a baseline of IT Governance. The fact that this scientific framework is used in practice and accepted by the market, forms the main argument for research based on this best practice. The research method of assessing interventions via an GSS expert panel, based on a Likert scale from -5 to 5, is therefore part of this research. Primarily to compile a weighted set of core security interventions for the mid-markets and to elaborate, based on a ranging scale, which intervention contributes to being (non) effective or (not) easy to implement for mid-markets in order to increase the security maturity.

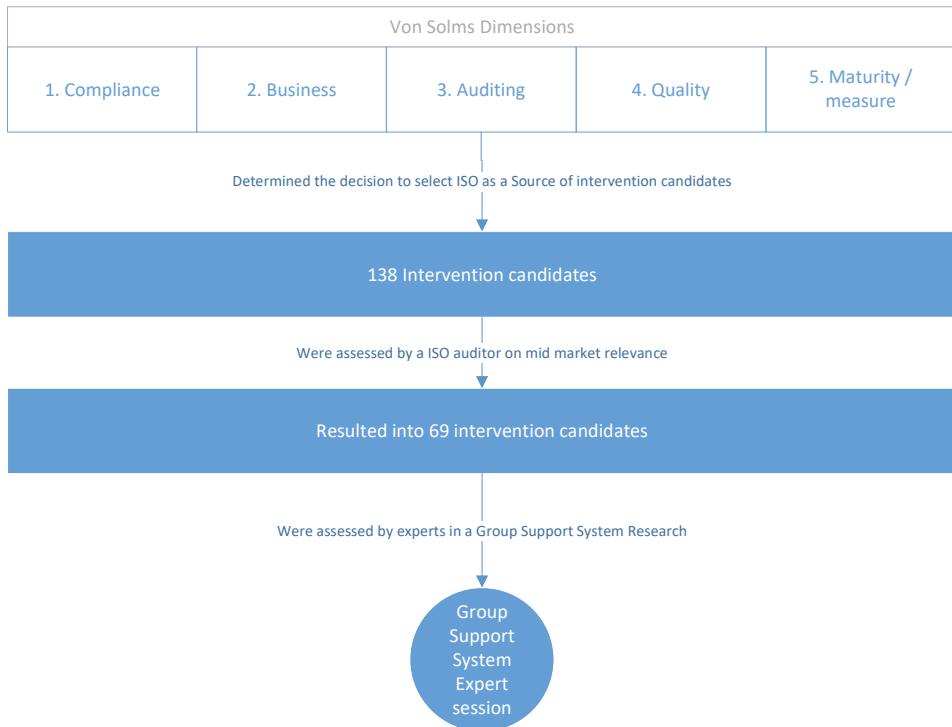


Figure 28: Preselection of intervention candidates.

FIRST STEP IN THE SESSION

An exercise made the experts familiar with the facilitating GSS. Experts were asked what they would bring to a deserted island. Firstly, the participants summed up a number of items. Secondly, the list of items was shown on the screen and the chauffeur categorised the outcome. Then, the items were ranked according to the amount of time the selection had taken. This exercise showed the participants how the system worked. They could also experience the speed of generating, originating, evaluating and analysing. The experts could get an idea of how to read, interpret and decide on core BIS interventions. Then a brief explanation was done that the 69 interventions were based on ISO on the basis of existing literature. The objective was to give the experts insights into the researcher's intervention selection.

An important step in selecting the core interventions was to have the expert judge the presented 69 interventions and generate the interventions that they find important. This was important because:

- New insights into the phenomena of security interventions were generated;
- Justification of these new insights. Why does an expert find these newly generated interventions important for this segment?;
- What is the extra value of these new interventions that the initial research phase overlooked?

Table 3: Expert panel characteristics.

	POSITION	PRACTITIONER	SCIENTIST	AUDITOR	TEACHER
1.	Security Manager (IT auditor (RE)) at a bank with 8000 employees	Y	N	N	N
2.	CISSP, CISM, CISA, security consultant and ISO27001 lead auditor trainer	Y	N	Y	Y
3.	Master's degree level, accountant (RA) and IT auditor (RE)	Y	N	Y	N
4.	EDP auditor, security manager at insurance company, editor of an Information Security magazine (PvIB)	Y	Y	Y	Y
5.	PhD in security, business consultant. Author of the book Economic Evaluation of Information Security, editor of an Information Security magazine	Y	Y	Y	Y
6.	Master in Information Security Management, Information Security officer at University of Technology, teaches information security	Y	Y	N	Y

4.4.5 SCORING OF INTERVENTIONS ON EASE OF IMPLEMENTATION AND EFFECTIVENESS

A new set of potential interventions was generated. Twenty one interventions were added to the list of sixty nine interventions. The next step was to make a qualified selection of practicable interventions for the mid-market. In order to make interventions attainable, acceptable and applicable in practice, we distinguished two criteria. *Ease of implementation* and *Effectiveness*.

The experts weighted an intervention on these two criteria to a scale of -5 to 5. -5 represents a negative effect, 0 as neutral and +5 represents a positive effect.

The result was a list of all interventions carefully selected by experts on 2 criteria and automatically ranked based on the qualitative output. The deviations in weight were, if required, commented by the experts. This provided the research with new insights:

1. *New insights into the phenomenon of security intervention effectiveness and ease of implementation;*

2. It became clear why experts gave more weight to certain interventions;
3. Deviations in the view of an expert became clear.

This step provided a selection of interventions based on important mid-market acceptance criteria, derived from expert opinions. This provided new insights into the reasons for differences in views on practicality and answered the research question "Which of the identified BIS interventions are practical in such organisations?".

In this research phase we also quest to understand why mid-market may not adopt security interventions. During this research phase, the experts pondered the reasons, assumptions, hunches, objections and other forms of barriers to the implementation of security interventions by the mid-market. Through the use of GSS a variety of barriers were generated. This data was valuable once we want to test it in a later phase of the research, i.e. the mid-market survey questionnaire.

4.4.6 FINAL SELECTION OF BIS INTERVENTIONS

To effectively qualify, categorise and assess all 69 interventions a computer system was used. According to Silverman [75], the advantages of using a computer are "*Speed at handling large volumes of data, freeing me to explore numerous analytic questions and Improvement of rigour, including the production of counts of phenomena and searching for deviant cases*". Using a computer system enables to focus on questioning and exploring unexpected variables in outcomes. In this case 69 interventions were judged by 6 people on 2 criteria. In theory this meant that 828 feedback options needed to be recorded, coded, analysed, interpreted and reported by one brain. It also provides you with assistance in sampling decision. In this case 69 interventions were ranked on 2 criteria which led to a set of representative interventions that could be presented in the survey questionnaire. Figure 29 displays the GSS meeting process that was followed in this research step.

4.4.7 MAIN BARRIERS FOR MBIS ACCORDING TO THE EXPERTS

All barriers that arose during the expert panel research with GSS were categorised in 4 main barrier categories:

Management and organisation: Examples of barriers that address the management of the organisation or the processes and configuration of the organisation. Examples that where collected during the research were; no process in place; no priority; lack of management commitment; the issue does not appear on the management agenda; no direct business demand; no necessity; no strategy on IT and definitely not on security. All of these barriers are categorised in Management and Organization.

Perception and attitudes: Barriers collected in the category of 'perception and attitudes' are; overwhelming amount of security information from different angles leads to confusion; difficult to implement and maintain; seen as a cost; no strong belief in necessity; we do not have incidents so everything goes well; information security equals technology; customer does not ask for it; denial of problems, afraid to admit security holes, etc.

Knowledge and Skills: Barriers mentioned in this category are; too many compliancy demands from numerous bodies; complexity of the phenomenon; lack of insights into current security level; inadequate level of knowledge at IT department; security is an expertise on its own; huge dynamics of threats, on the one hand, and keeping up with these threats, on the other.

Budget refers to arguments that are related to money. Budget is the exhaustive terminology for everything related to the financial side of the security intervention investment. Just as we learned from the barrier 'management and organisation', we again deal with BIA-like barriers. It appears that business security and the intervention implementation suffer the same hurdles. Barriers that arise in this category are; security is seen as a cost instead of an investment; returns are not seen; difficulty of financially planning; lack of a dedicated budget.

Expert panel member EA mentioned during the panel session, and in earlier studies about the economic evaluation of information security, it is the lack of insights into future cost savings, derived from the prevention of losses due to information security breaches.

Other barriers that were not mentioned but are applicable all the same: no security project coherence and no security project portfolio management backed up with business cases (management & organisation) [246].

4.4.8 EXPERT PANEL DATA ANALYSIS

After identifying the deviations between the experts an analysis was performed. For this research section we analysed the interventions with the most significant variety or interesting feedback during the research.

Information Security as part of the business continuity plan scored 1.5 on effectiveness and 0.5 on ease of implementation. The deviation on its effectiveness was caused by the fact that this depends on the person who's assigned for this job. Some experts say that there are more effective ways to increase the security, while others say it is a prerequisite for any organisation. When we consider business continuity and avoid loss of revenue due to security breaches this intervention is vital, even though it scores very low on ease of implementation.

The intervention with a slight deviation was '**Creation of audit and log files**'. Main reason for this was that the pure security expert argument is that "you need to do something with it, otherwise it is a waste of megabytes or paper". The auditing and accountancy experts from

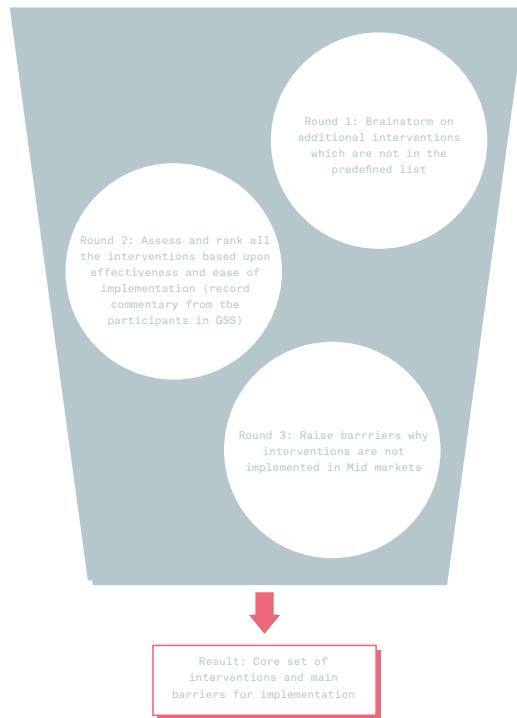


Figure 29: GSS expert meeting process flow

the panel confirmed the idea that it is necessary in order to be 'in control' and to have proof in case of incidents. Quote: "the audit trail is very important for financial auditors, because they have to test the working (test of controls)".

Performing IT risk analysis. Experts' opinions vary in the complexity of this intervention.

One experts said it is hard to do this very thoroughly and you need to master all the economic evaluation criteria. Others say it is 'wet finger work', as long as it is done. 'That's the most important thing'.

Non-disclosures. According to the experts this is a false sense of security. It is really hard to constantly maintain and ensure, especially with temporary personnel, interns, factory workers, etc.

Reporting security vulnerabilities. This variety in experts' opinion was because some experts say this required knowledge and expertise in order to assess technical vulnerabilities, this explains the low score on ease of implementation. Others say you can in-source this expertise but it is a necessity in order to know where which intervention is necessary, that explains the high score on effectiveness.

Security awareness training. All experts agree this is very effective (3.67) primarily because human errors lead to most of the security breaches. When you increase the awareness of security you decrease the potential change to human errors. Experts argue that awareness training need to be mandated by management and management is not involved and therefore security awareness does not reach the agenda or priorities. **Separation of duties** led to differences of opinions by the experts. Some say it is very hard to realise (score 0 on ease of implementation), other say it is a necessity from accounting perspective. Quote: "segregation of duties has to be implemented adequately. In the case of insufficient segregation of duties it has a negative influence on the auditor's report. Qualification the audit report". All experts judge this intervention to be effective (3.17).

Managing user access rights caused deviations of 66% because it scores 0.17 on ease of implementation. Mainly because it is expensive and requires a lot of knowledge. It scores 4.33 on effectively mainly because it takes care of a lot of security issues. Quote from the experts: "is necessary to avoid 'doublers in function'"

Identifying applicable laws and legislation. According to the experts this is a prerequisite for every organisation. But it's quite hard when you don't have the necessary knowledge or expertise.

4.4.9 RELEVANT INTERVENTIONS

During the expert panel session input was collected to take into consideration in the next research phase, the survey questionnaire aimed at the mid-market segment. Experts suggested that the following interventions must be included in the survey questionnaire in order to have an exhaustive list of relevant interventions:

Change management on security devices: experts argued that "*this is needed for applications with financial effect for the annual accountants/ financial figures*". And in order to be in control for compliancy means.

Protection of Information and securing privacy information. This intervention is a prerequisite for any organisation in the EU. Since strict regulations need to be followed, all organisations need to have this intervention in place; Since the subject of this research is business security an intervention addressing **business continuity** is appropriate;

Management of technical vulnerabilities is a necessity in order to be in control of outbreaks or security breaches. In order to be in control, organisations also need to have a plan which can only be effective when an organisation knows what to safeguard;

Risk and impact analysis. In order to invest in security intervention, an organisation needs to know to what extent to safeguard their business (information) and what the related costs of potential breaches are. The only way to do this efficiently is to conduct business, risk and impact analyses;

Separation of duties. According to the experts, this is a very effective intervention but difficult to implement. One expert said: "*segregation of duties has to be implemented adequately. In the case of insufficient segregation of duties it has a negative influence on the auditor's report*". Separation of duties is the first method to avoid security problems and the best way to track who has done what (audit trail);

Identification of applicable law. This intervention was substantiated by the experts as "compliance with laws and regulations is essential for an enterprise to be in control".

Table 4: Top interventions according to experts

	INTERVENTION	PERCEIVED EFFECTIVENESS (-5 TO +5)	PERCEIVED EASE OF IMPLEMENTATION (-5 TO +5)*
1.	Management commitment to information security	5	4.33
2.	Protection against malicious and Mobile Code	3.55	4.17
3.	Systems classification	3.33	3.5
4.	Cryptographyc controls	3.83	2.67
5.	User identification and authentication	3.67	2.67
6.	Screening before employment	3	3.17
7.	Information backup	4.83	1.33
8.	Equipment maintenance	2.67	3.17
9.	Access Control Security	4.4	1.2
10.	Disposal of media	3.6	1.8
11.	Allocation of information security responsibilities	3.17	2.17
12.	Creation audit and logfiles	3	2.33
13.	Secure Log-on procedures	3	2.33
14.	Use of supplier guidelines	2.4	2.8
15.	Mission, vision, strategy of buisness seen as a whole	3.17	2
16.	On-line transactions	3.83	1.33
17.	Management of special privileges	3.33	1.83
18.	Equipment sitting and protection	3.33	1.67
19.	Monitoring and review of third party services	3.17	1.67
20.	Learning from security incidents	2.67	2.17

* A scale of -5 to +5 is used, -5 being not contributing, 0 being neutral and +5 being highly contributing

The entire GSS session was recorded on film and reported into a meeting report format. This can be found in the appendices and can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

4.5 PERFORMING THE DELPHI RESEARCH VIA A SURVEY

The expert panel research produced a wealth of valuable information on essential interventions, carefully assessed on effectiveness and ease of implementation based on a proven scientific method. A core set of interventions and insight in possible barriers evolved from this research. With this information a survey questionnaire was compiled to conduct data about the mid-market state of security maturity. This survey was conducted during the second quarter of 2010 and was sent out to 50 organisations from which 40 participated. The objectives of the blind mid-market survey questionnaire, as proposed in chapter 2 to avoid group influence, were:

1. Test the assumption that organisations do indeed want to increase their security maturity level (based on COBIT maturity model);
2. Test organisations maturity levels and ambition levels;
3. Test if organisations are aware of applicable law and legislation;
4. Measure and test which essential interventions are enforced;
5. Measure and test barriers;
6. Ask for feedback (qualitative) on the interventions which contribute most to their opinion.

Quantitative research (Yes/No questions) was applied in order to collect data that provides direct insight into the current status of the participating organisations, compared to the desired state of information security maturity. This also provides direct insight into whether organisations actually want to increase their maturity levels. Some open questions are of a more qualitative nature, which enables participants to provide feedback that can be useful in building up a complete picture of security.

4.5.1 COMPOSING THE SURVEY QUESTIONNAIRE

In the previous section the interventions that needed to be validated by the mid-market organisation was compiled by the experts. In order to get more contextual information about the organisations and their variety of industry the respondents were asked some additional questions:

1. What sector is the mid-market organisation part of?
2. In order to test whether the organisation is aware of applicable law or legislation one question addresses that item.
3. In order to plan business information security, I would like to explore whether organisations actually have the ambition to increase their security maturity. I assume they do but a

- question addressing this item is included for the sake of the reliability of the research.
4. In order to know where organisations are at this moment in time (baseline), I want to explore how representatives of organisations judge their own organisation based on the 5 scale maturity model of COBIT.

I intentionally included this question, and received answers on applied interventions. That gave me a testing method to test the actual maturity level of that organisation and the reliability of the respondents. For example, if he/she judges the organisation's level at 4 or 5 and core interventions are not applied, one can doubt the reliability of the respondent and delete the answer from the results.

5. Respondents were asked which intervention contributes most to increasing security maturity in their view. They were asked to motivate their answers, leaving room for interesting arguments that helped me to get a better picture of mid-markets view on security.
6. Participants were also asked for additional feedback (on items that they had missed in the session).

The compiled research questionnaire was carefully reviewed by KS a PhD, and lecturer in academic research techniques at Utrecht University of applied sciences. Then the list was sent to four sample participants in order to test the methodology, the completeness of the list and the clearness of the questions. I wanted a non-security person to be able to understand the questions, especially because the intended outcome must be accepted by business managers as well. The only way to achieve this result is to have a clear and consistent business terminology. Mentioned below are the most relevant questions. For the complete survey questionnaire see appendix.

4.5.2 SURVEY PARTICIPANTS

The definition of a mid-market is an organisation with between 100 and 2500 computer systems. To conduct a survey within 40 organisations I have a substantial number of organisations representing this mid-market segment. To get feedback on relevant questions, and to motivate the participants, I have sent approximately 50 people a personal email with an invite to participate in my research. Eventually 40 responded to participate. Screenshots of the original email are in the appendix and can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

After the participants accepted the invitation to participate, a second email was sent out with instructions about the survey and how to fill in the questionnaire. Also a guiding document on how to interpret the maturity model (based on COBIT) and the barriers (derived from the experts' opinion). Emphasis on the deadline on when the participants needed to fill in the questionnaire was also added in this mail. Screenshots of the original email are in the appendix, accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc..>

4.5.3 SURVEY QUESTIONNAIRE (WEB-BASED)

When the participants received this email they were guided to a website where the questionnaire could be filled in. The survey was guided with a brief explanation on what the purpose of the questionnaire is and how people need to fill in the form. The second part of the questionnaire includes interventions and their barriers. Brief explanations guided the participant into the questionnaire.

"Research has shown several interventions that are important for maturing the information security. Below is a list of the top interventions Please indicate on this list at each intervention whether your organisation enforce this intervention completely. If it does, then select Yes. If your organisation does not enforce or only partially enforce the intervention then select No and at the next question give the reason."

After receiving all the participants' data, a broad collection of this data was put into a database in order to do a thorough analysis. The complete survey data is enclosed in the appendix. A summary of the most relevant data that could answer most of the important research questions is presented in under mentioned figures and tables.

4.5.4 SURVEY PARTICIPANTS AND THEIR INDUSTRY

The first selection on the data collection was made on industry type. Additional a timestamp was added in order to assure authenticity of the participant in combination with his/her personal ID. This personal ID referred to organisations names and contact details of the participants. In order to assure confidentiality that data was kept separate. In the Table 5 all participating companies were identified based on a personal login code which was provided via email. The time of login was registered. The participants were asked in which industry their company is active.

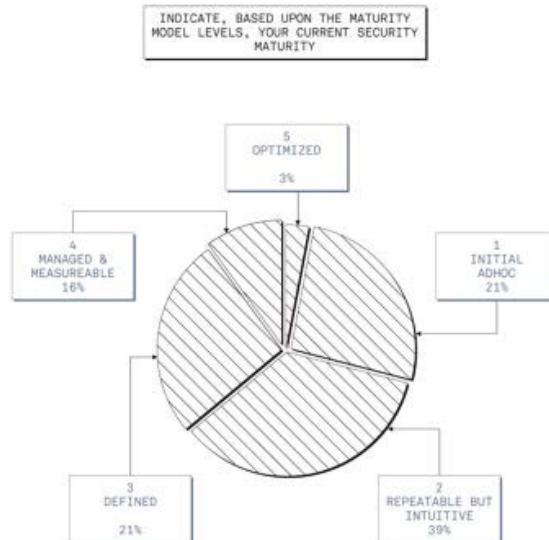


Figure 30: Indication of the maturity level in 2010.

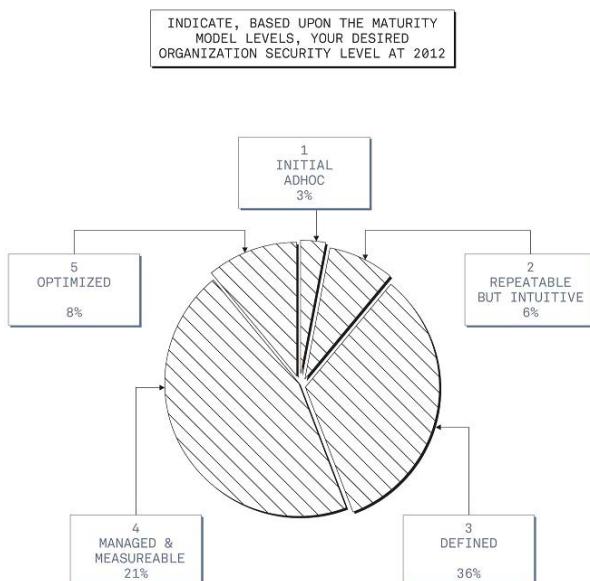


Figure 31: Indication of the desired maturity level in 2012.

Table 5: Mid-market sectors and current versus desired maturity state.

TIMESTAMP	PLEASE FILL IN YOUR PERSONAL CODE	WHAT SECTOR IS YOUR ORGANISATION IN?	DOES YOUR ORGANISATION HAVE TO BE COMPLIANT TO CERTAIN RULES, LAW AND/OR LEGISLATION?	INDICATE, BASED ON THE MATURITY MODEL LEVELS, YOUR CURRENT SECURITY MATURITY LEVEL	INDICATE, BASED ON THE MATURITY MODEL LEVELS, YOUR DESIRED ORGANISATION SECURITY MATURITY LEVEL AT 2012
3/5/2010 10:50:04	QuRKaZa120X27	Media	Ja (Yes)	2 Repeatable but intuitive	
3/5/2010 11:05:59	QuRKaZa120X4	Detailhandel (Retail)	Ja (Yes)	3 Defined	
3/5/2010 11:42:53	QuRKaZa120X35	Government (Overheid)	Ja (Yes)	2 Repeatable but intuitive	
3/5/2010 11:58:49	QuRKaZa120X48	Installatie techniek	Ja (Yes)	1 Initial/ Ad hoc	
3/5/2010 14:12:51	QuRKaZa120X7	Health Care (Gezondheidszorg)	Ja (Yes)	2 Repeatable but intuitive	5 Optimized
3/5/2010 16:32:50	QuRKaZa120X72	Government (Overheid)	Ja (Yes)	2 Repeatable but intuitive	4 Managed / measurable
3/5/2010 22:09:42	QuRKaZa120X51	Government (Overheid)	Ja (Yes)	3 Defined	4 Managed / measurable
3/6/2010 13:38:27	QuRKaZa120X31	Health Care (Gezondheidszorg)	Ja (Yes)	5 Optimized	5 Optimized
3/6/2010 15:06:34	QuRKaZa120X6	Finance (Financiële dienstverlening)	Ja (Yes)	4 Managed / measurable	4 Managed / measurable
3/8/2010 7:01:06	QuRKaZa120X5	zakelijke dienstverlening	Ja (Yes)	3 Defined	4 Managed / measurable
3/8/2010 9:42:17	QuRKaZa120X26	Logistiek	Nee (No)	3 Defined	4 Managed / measurable
3/8/2010 12:43:48	QuRKaZa120X50	Government (Overheid)	Ja (Yes)	1 Initial/ Ad hoc	2 Repeatable but intuitive
3/8/2010 12:47:37	QuRKaZa120X3	Health Care (Gezondheidszorg)	Ja (Yes)	1 Initial/ Ad hoc	3 Defined
3/8/2010 15:55:52	QuRKaZa120X49	Government (Overheid)	Nee (No)	3 Defined	4 Managed / measurable
3/8/2010 22:44:15	QuRKaZa120X42	Health Care (Gezondheidszorg)	Ja (Yes)	2 Repeatable but intuitive	4 Managed / measurable
3/9/2010 12:00:56	QuRKaZa120X9	Legal	Nee (No)	4 Managed / measurable	5 Optimized

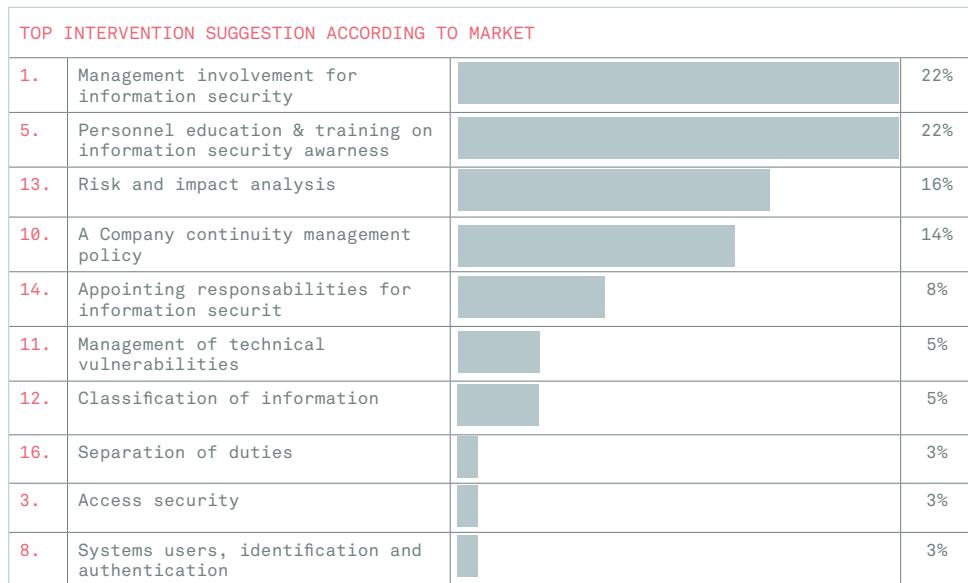
3/10/2010 13:18:21	QuRKaZa120X40	Retail	Nee (No)	2 Repeatable but intui-tive	3 Defined
3/11/2010 11:00:45	QuRKaZa120X10	Onderwijs (Edu-cation)	Ja (Yes)	3 Defined	4 Managed / measurable
3/11/2010 14:26:43	QuRKaZa120X8	Retail	Ja (Yes)	2 Repeatable but intui-tive	4 Managed / measurable
3/11/2010 16:40:35	QuRKaZa120X24	Industrie (in-dustry)	Nee (No)	2 Repeatable but intui-tive	4 Managed / measurable
3/12/2010 11:31:46	QuRKaZa120X73	Maatschappeli-jke opvang en welzijn (Social care)	Ja (Yes)	3 Defined	3 Defined
3/15/2010 15:12:35	QuRKaZa120X71	Finance (Finan-cieele dienst-verlening)	Ja (Yes)	3 Defined	4 Managed / measurable
3/15/2010 15:34:23	QuRKaZa120X39	Internet Retail	Ja (Yes)	3 Defined	4 Managed / measurable
3/15/2010 18:52:52	QuRKaZa120X52	Food	Ja (Yes)	1 Initial/ Ad hoc	3 Defined
3/16/2010 0:34:34	QuRKaZa120X29	Health Care (Gezondhe-idszorg)	Ja (Yes)	1 Initial/ Ad hoc	3 Defined
3/16/2010 11:21:00	QuRKaZa120X61	Government (Overheid)	Ja (Yes)	1 Initial/ Ad hoc	3 Defined
3/16/2010 11:26:31	QuRKaZa120X11	Finance (Finan-cieele dienst-verlening)	Ja (Yes)	4 Managed / measurable	4 Managed / measurable
3/16/2010 11:26:48	QuRKaZa120X33	Pharmaceutical	Ja (Yes)	2 Repeatable but intui-tive	4 Managed / measurable
3/16/2010 11:39:44	QuRKaZa120X21	Housing (Onro-erendgoed voor-ziening)	Ja (Yes)	2 Repeatable but intui-tive	3 Defined
3/16/2010 12:13:22	QuRKaZa120X18	Agri Culture	Ja (Yes)	1 Initial/ Ad hoc	1 Initial/ Ad hoc
3/16/2010 12:22:31	QuRKaZa120X25	Government (Overheid)	Nee (No)	4 Managed / measurable	4 Managed / measurable
3/16/2010 12:26:26	QuRKaZa120X46	retail food	Ja (Yes)	2 Repeatable but intui-tive	4 Managed / measurable
3/16/2010 12:30:38	QuRKaZa120X35	Government (Overheid)	Ja (Yes)	2 Repeatable but intui-tive	3 Defined
3/16/2010 15:01:25	QuRKaZa120X59	Onderwijs (Edu-cation)	Nee (No)	2 Repeatable but intui-tive	3 Defined
3/16/2010 20:00:16	QuRKaZa120X19	logistiek & financiële dien-stverlening	Ja (Yes)	4 Managed / measurable	4 Managed / measurable

3/17/2010 9:40:51	QuRKaZa120X47	Finance (Financiële dienstverlening)	Nee (No)	2 Repeatable but intuitive	3 Defined
3/18/2010 8:44:02	QuRKaZa120X100	Finance (Financiële dienstverlening)	Ja (Yes)	2 Repeatable but intuitive	3 Defined
3/18/2010 10:01:49	QuRKaZa120X54	Government (Overheid)	Ja (Yes)	4 Managed / measurable	5 Optimized
3/18/2010 14:18:58	QuRKaZa120X70	Government (Overheid)	Ja (Yes)	1 Initial/ Ad hoc	2 Repeatable but intuitive
3/18/2010 14:46:32	QuRKaZa120X22	Industrie (Industry)	Ja (Yes)	2 Repeatable but intuitive	3 Defined
3/19/2010 10:37:10	QuRKaZa120X15	Recycling	Ja (Yes)	2 Repeatable but intuitive	3 Defined

4.5.5 ANALYSIS OF SURVEY DATA

After capturing the data via a secure web-based tool we analysed the data and elaborate some important findings.

Table 6: Top intervention suggestions according to mid-market organisations.



Most researched mid-market organisations suffer from a lack of management commitment, even though research institute literature indicates that C-level people (Chief level) see the value of increasing their security levels to enhance customer trust, employee loyalty and

company integrity, etc. [11]. The mid-market indicates this intervention as the number one contributing intervention to increase their business security maturity.

A total of 83% of the mid-market companies do not educate and train personnel on security awareness, even though 22% of the respondents indicate this intervention to be the second most contributing intervention of increasing their own information security maturity level. It scores high on wish list and is seen as a necessity. Perception is the biggest barrier for implementing this intervention. The paradox is that the perception of the effectiveness of training and educating stands this important barrier in the way.

A small proportion (34%) have risk and impact analysis enforced. This intervention is necessary to adequately know what you need to protect. The mid-market recognises this and ranks this one third on their suggestions to increase their business security. They recognise the need to know the value of the data and information in order to financially justify the implementation of an intervention. Top barrier in this respect is perception and knowledge (32%) since most of the people (e.g. experts) say this could be seen as complex and requires specific economic expertise.

Budget is listed as the most irrelevant barrier, even though today's economic climate seems to indicate the opposite. It is also interesting that so far management has not been involved by many organisations. Security is perceived as a highly complex topic, the result of which is that essential interventions are not being enforced.

Conclusive we can state the organisations under review are unable to identify essential interventions and struggle because of insufficient knowledge and skills, even though the absence of implementation of core interventions could seriously endanger the continuity of these organisations. On the basis of these findings, it can be argued that communication between business and security is misaligned.

4.6 CONCLUSIONS OF THIS STUDY INTO BIS MANAGEMENT INTERVENTIONS

Experts created a top list of interventions from ISO 27002, based on the practicality of each intervention. As a conclusion to the survey research performed in the mid-market segment, I encountered a willingness to implement certain interventions in order to increase security maturity. These were not enforced due to several reasons. As a conclusion to the mid-market survey I observed:

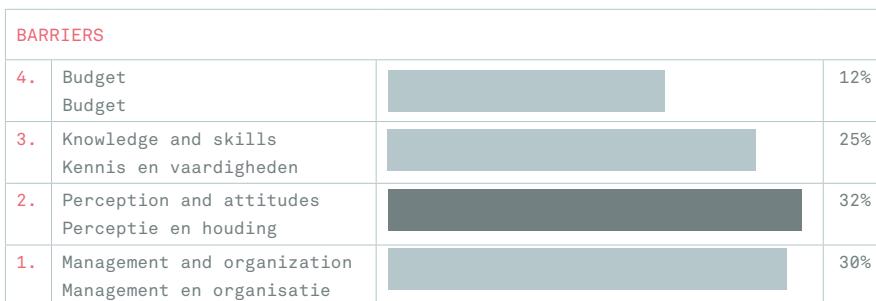
- The barriers "management and organisations" as well as "perception and attitudes" are two categories scored high in the survey. These were also raised by the experts during the panel as main barriers.
- Mid-market organisations state in the survey that involving management would raise their security maturity level. On the other hand, security is perceived as a complex topic and

this contradicts the above. How can a security person with the wrong perception advise management on interventions contributing to maturity enhancement?

- The survey showed that 22% of the mid-market suggest that 'training and educate personnel on awareness' contributes most to security; this equals the opinion of experts according to the expert panel research. The main question remains how they want to do that in the face of insufficient knowledge and skills.
- The experts mentioned during the expert panel research phase that the overwhelming number of applicable laws and frameworks might suffocate the mid-market. This seems to be acknowledged by the fact that perception is the biggest barrier and 20% of the organisations do not know that there is indeed applicable law. The mid-market has difficulties identifying these, according to the survey outcome.
- Budget is raised as a barrier by the experts but not listen as an intervention, for example "more money". In contradiction to the barrier perception where the intervention is training and educating on awareness. And for the barrier "management and organisation", the intervention management involvement is suggested by the mid-market organisations.
- According to the survey "perception and attitudes" is the biggest barrier to the implementation of the third most contributing intervention, risk and impact analysis. Important questions for mid-market organisations remains open, i.e. by whom they want to have this risk and impact analysis performed, since they consider it to be complex and lack the necessary knowledge and skills.

In conclusion, we can state that filling in the survey questionnaire has raised the awareness of mid-market participants. Responses to open questions such as "that's a good idea", "needs to be developed", "good idea to apply this" proved this.

Table 7: Barriers according to companies in the mid-market



4.7 CONTRIBUTION & RECOMMENDATIONS

The presented list of interventions forms the first step towards the conceptual framework for BIS, and list of interventions for mid-market organisations in order to improve business information security maturity. A carefully selected list of interventions presents those interventions that are most effective and easy to implement for a market that, according to the performed survey, struggles with the enforcement of essential interventions. By making use of a combination of the ISO best practices and for example the COBIT maturity model organisations can have better insights into the interventions they have applied as well as those they need to apply in order to achieve a certain maturity level. Translating the most important conclusions of the research into mid-market specific recommendations in order to increase their security maturity, by applying a framework (of interventions, suggested maturity model, organisational preconditions) the research primarily recommend mid-market organisations to:

1. Identify applicable (mid-market) laws and legislation.
2. Perform risk and impact analysis in order to justify the implementation of necessary interventions in order to achieve the desired security maturity level.
3. Apply relevant norms in order to comply with law, legislation or regulations or a framework that is derived from these norms, for example COBIT.
4. Involve management about the business impact of not having these essential interventions in place.
5. Increase the awareness of security throughout the organisations since human error is a predominately cause. Train and educate with focus on the correct perception about security on the technical as well as the business side of the organisation.
6. Measure and monitor all potential technical and organisational vulnerabilities (security assessments) as a continuous process in order to be in control and achieve the desired level of security maturity.
7. Continuous maintain knowledge and skills that are essential to keep being "in control".

4.8 LIMITATIONS OF THIS STUDY

A limitation of this study is the use of a set of predefined interventions of ISO. Although they are accommodated through the GSS session with additional insights and new interventions it is still limited. This can be solved by the continuous research into new interventions or practices, perhaps gained in other disciplines such as risk management, business management, etc. The ISO 27K interventions are also limited to mainly the tactical level of management of information security, limited to the strategic level (Board of Directors and executive management of Information Security). This argument of mainly management focus within the Information Security field was raised by Von Solms [247] and proposed the involvement of the strategic level [71], in the Governance of Information Security. This is also recognised and addressed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [113]. As important initiative the ISO committee established the

standard for proper Governance of IT (ISO38500)²⁴ in 2008. The ISO38500 was later on examined and implemented into the COBIT5 for Information Security framework [56], still principally influenced on IT practices instead of Corporate Governance.

Another limitation of this study is the sample size and the characteristics of the respondents. The sample size of n=40 seem limited for quantitative analysis but is fairly large for a qualitative analysis. The sample was random, and in random sampling the *samples are selected by a chance-based method that gives all observations an equal likelihood of appearing in the sample* [248]. If the objective is to perform statistical analytics on this data, the sample size needs to be larger and have a certain amount of shared characteristics. This increases the generalizability of sample results, e.g. external validity. This also requires a more valid representation of the participants in this research. In this case organisations could not be interviewed as such, but rather individuals in different roles (IT managers, security managers, etc.). Thus it is hard to perform any statistics on this mainly qualitative dataset, which has too much variation in the characteristics of the respondents. The objective of this research was to examine and determine parameters to be built into the artefact. Further research can be performed on organisations, which are mostly represented via individual respondents with close-to-identical characteristics (e.g. function, education, certifications, hierarchy in the organisation, budget span, span of FTE control, etc.) and therefore eligible for statistical inference. The population of these 40 organisations with different respondent criteria is too random in order to sufficiently generalise the data. This is why the recommendations for mid-markets raised in this chapter are limited in their generalizability and are subject to the above- mentioned limitations.

The main objective of this chapter was to examine the first iteration of potential parameters. These parameters evidently change due to time, technology and business requirements and require continuous assessment. Again, the aim here is not, in this initial phase, to be exhaustive in terms of interventions or requirements.

²⁴ ISO/IEC 38500:2008 provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations. The ISO38500 was amended in February 2015 (Source iso.org)

5

EXPLORING GOVERNANCE PRACTICES FOR IMPROVING THE Maturity OF BUSINESS INFOR- MATION SECURITY

This chapter provides an extensive, in-depth literature survey of governance practices relevant for the improvement of BIS maturity. It establishes a rigorous process, based on the proposed research techniques in chapter 2, of literature research and expert validation, leading to the establishment of a core set of governance practices that are relevant for Boards of Directors, which can be used in the next research phases.

This chapter was published and presented in 2013 on the 46th Hawaii International Conference on System Sciences (HICSS) in Hawaii United States under the title: Group Support Systems Research in the Field of Business Information Security; a Practitioner's View.

5.1 INTRODUCTION

In the previous chapter we have examined potential management interventions for the improvement of BIS maturity. The result is a conceptual framework for BIS. This chapter picks up the identified need for examining BIS Governance practices since they seem to be lacking in current bodies and have been addressed by the mid-market respondents as relevant to have for the improvement of BIS. This chapter presents the findings of a second research phase, as a follow-up to Chapter 4, and presents a comprehensive, thoroughly selected core set of BISG practices to be used by practitioners in the business environment. It elaborates the Design Science Research process of researching the literature (Rigor Cycle) on practices, scrutinise the latter via a GSS expert panel research (Design cycle) and present them as requirements for the artefact in the later chapters. The objective is to examine BIS Governance practices that can be part of the conceptual BIS framework mentioned in the first chapter. In this part we use the proposed research methods of literature survey, to collect a list of governance practices from other domains that can form an inspiration and assess that complete list via experts in the field. Thus, we do not focus on validating this with mid-markets, and purely use experts.

5.2 BACKGROUND OF THE RESEARCH PROJECT

In the previous chapter a conceptual framework for BIS interventions was presented [249]. This set of security practices proposed by the group of experts and subsequently validated by organisations, showed a lack of attention to governance practices. These findings are supported by literature [250], [209], [247]. The lack of attention to governance practices is a problem for two reasons: firstly, governance is a necessity for mandating security management [239]. Secondly, security ought to be part of the organisational culture but is not [251], [194]. The aim of this research project is to develop a framework supported by a large-scale and longitudinal Group Support System to monitor, evaluate and direct business security governance with small teams (e.g. Boards of Directors, Executive Management Teams). The framework can be used as input for requirement setting in the design artefact. Therefor separate –requirement- design questions are formulated in this chapter.

The first section of this chapter consists of definitions within the BISG topic. The second section deals with a review of recent academic and practice-oriented literature relevant to BISG. A number of experienced security experts were subsequently asked to assess this large amount of data (228 practices). The experts selected, organised and ranked the practices via GSS. The results enabled further examination of the factors influencing Governance Practices. These findings will serve as potential input for developing a framework to monitor, evaluate and direct BISG.

5.3 RESEARCH METHOD & FINDINGS

5.3.1 LITERATURE REVIEW

The current research project started with an extensive literature study, capturing all literature on Governance Practices relevant to the topic of Business Information Security Governance. The reviewed governance practices are;

1. Corporate Governance practices;
2. Risk Governance practices;
3. Enterprise Governance of IT practices and
4. Information Security Governance Practices.

1. CORPORATE GOVERNANCE PRACTICES

Approximately 50 best practices from the **Corporate Governance** discipline were examined. The major sources of origin of these practice are: The OECD Principles of Corporate Governance [252]; the Commonwealth Association for Corporate Governance [253]; Internal Control Guidance to Directors, Turnbull Report [254]; The Financial Reporting Council (FRC) Combined Code [255], The King Report on Corporate Governance for South Africa [256]; Bank for International Settlements (BIS). Basel principles for enhancing corporate governance [257], Security and Exchange Commission (SEC) add-ons to SoX, Commission on Public Trust and Private Enterprise 2003. Most of them can be found in the Corporate Governance Book (Oxford University Press) which covers all international Corporate Governance codes [59].

2. RISK GOVERNANCE PRACTICES

A major component of practising good governance is the **Risk Governance** discipline. Insufficient Risk Governance and management have enormous consequences for all major stakeholders [20]. The judgement and management of IT-related risks has become increasingly important to the success of businesses [197]. For the assessment of all relevant Risk Governance practices, I examined literature from: COSO's Enterprise Risk Management Integrated Framework [258]; COSO's "Embracing Enterprise Risk Management": Practical Approaches for Getting Started [259]; COSO's "Where Board of Directors Currently Stand in Executing Their Risk Oversight Responsibilities" [31]; King's Report on Corporate

Governance for South Africa – 2002 [256], and Douglas Hubbard's study on Risk Management Failures. A total of forty Risk Governance practices were selected.

3. IT GOVERNANCE PRACTICES

Forty **IT Governance** practices were selected from several sources: IT Governance Institute, "Information Risks: Whose Business Are They?" [18]; De Haes & Van Grembergen's "Practices in IT Governance and Business/IT Alignment" published in ISACA's journal (Information Systems Audit and Control Association); Weil & Ross' "IT Governance" [260] and De Haes & Van Grembergen's book "Implementing Information Technology Governance; Models Practices and Cases" [217] and Van Grembergen's "Strategies for Information Technology Governance" [108].

4. INFORMATION SECURITY GOVERNANCE PRACTICES

During the selection of the literature, numerous academic and practice-oriented sources were investigated, mainly to judge their appropriateness for ISG practices. I investigated a large number of resources on **Information Security Governance**, because this discipline is the most closely related to Business Information Security Governance (BISG). I investigated sources from an international context to avoid missing out on important developments worldwide; multi-sources (research institutes such as IDC and Gartner) and academic journals and books (from Harvard Business Press, Springer, and Wiley). The research also focused on best practices institutes such as ISACA, ITGI, ISF, SABSA, etc., and other communities practising Security Governance. An examination of highly respected and well-established literature sources resulted in a selection of 98 practices. The major literature sources are: the 2004 Corporate Governance Task Force Report of the National Cyber Security Summit [261], chapters "Information Security Governance and Responsibilities of the Board of Directors/Trustees"; De Haes & Van Grembergen's "Practices in IT Governance and Business/IT Alignment" (in ISACA's journal, 2008) [105]; Von Solms's, "The 10 deadly sins of information security management" [105] and other major relevant sources on the BISG topic [262], [22], [263], [63], [264], [209], [52].

The practices that were examined and selected may be potentially applicable for BISG. In order to delete doubles, vaguely articulated practices and so on, a thorough validation of all 228 practices by an expert panel is essential. Before presenting the total of 228 practices to the expert panel, I first structured them by marking them with their origin (source of literature) as well as their discipline (RG=Risk Governance; CG=Corporate Governance; ITG=IT Governance; ISG=Information Security Governance). In addition, I organised the candidate practices by marking them according to De Wit & Meyer's Strategy Theory [216]: "*Organisational Structures, Processes & Relational Mechanisms*" respectively. In the current research project, I use a more exhaustive terminology when discussing Relational Mechanisms because the term addresses more than just the culture of an organisation such as respect, attitude or behaviour. De Wit and Meyer's theory was successfully applied in other studies [187] and was applied by Van Grembergen and De Haes in the development

of a framework for the Enterprise Governance of IT. This framework and the three major components for compiling a set of BISG practices are applied in the current research project. During the literature review all 228 practices were marked including marks for Process Contributing Practices (P), Structure Contributing Practices (S) and Relational Mechanisms Practices (RM). The experts were presented with a complete list of 228 practices. They were asked to analyse and investigate this list which was defined as the "Complete List of Governance and Management Practices".

5.3.2 EXPERT PANEL

EXPERT PROFILE AND TITLE	EXPERTS CHARACTERISTICS AND DISCIPLINES						
	POSITION	MANAGER	PRACTITIONER	BUSINESS ADVISORY	AUDITOR	CONSULTANT	EXPERTISE IN YEARS
BSc RE CISM	Security Officer at Bank	Y	Y	Y	Y	N	>20
BSc CISSP CEH	Security Architect Telco	N	Y	Y	N	Y	>10
MSc RE	Manager at IT Advisory	Y	Y	Y	Y	Y	>15
MSc BSc CISM	Security Consultant	N	Y	Y	Y	Y	>20

In order to organise, assess and rank the practices, a Group Support System (GSS) was used in order to facilitate the expert focus group. Quality is preferred over quantity since I wish to achieve a thoroughly analysed and ranked set of practices according to true experts. Four experts were selected according to the following criteria: they have a BA or MA degree in Information Systems, completed with industry certificates i.e. Certified Information Security Manager (CISM); Certified Ethical Hacker (CEH); Register EDP auditor (RE). The chosen experts have over 10-year experience in Business Information Security; they are full-time practitioners in Business Information Security and have (had) a link to the strategic management of organisations. These four experts are perfectly situated to select and rank this huge amount of data in the literature which makes their assessments highly relevant. Due to their multidisciplinary backgrounds (see table 1), their opinions are generalisable across numerous domains and different types of industries. The group size is similar to a Board of Directors or Executive Management Team and will therefore enable us to test on collaboration in small teams with large data sets.

5.3.3 RESEARCH FINDINGS

All 228 practices relevant to the topic of Business Information Security Governance were examined via GSS by the four experts. Because of the time available for assessing and organising the items, each expert pre-assessed each of the four data sets and passed it back to the group (carousel concept). Short commentaries were given within GSS to justify the deletion or undoubling. See below for some examples of experts' judgements and opinions on certain practices. The practices that are potential candidates for further research and with a wide variety of opinions as well as relevant critics are discussed below. The entire session was recorded and documented and can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

50 practices from the Corporate Governance literature were assessed and organised by experts' opinion via GSS. One of the first and most essential ones is the role of the stakeholder:

CG P Determine the Role of Stakeholders. The corporate governance framework should recognise the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises. Source: The OECD Principles of Corporate Governance, 2004 extracted 24 September 2011 from www.oecd.org

- The experts' commentary on this Corporate Governance practice is that it is identical to the stakeholder analysis mentioned by numerous other sources. They also comment that this one is focused on financial institutions. One of the experts also commented that the role of the stakeholder is often regulated in laws.

CG RM Adequate Knowledge on protection of Intellectual Capital. Ensure the motivation and protection of intellectual capital intrinsic to the corporation, ensure that there is adequate training in the corporation for management and employees, and a succession plan for senior management (principle 12) Commonwealth Association for Corporate Governance [253]

- The experts commented that the wording of these practices was rather vague. They mentioned that awareness is the key word here. According to the experts, these practices can be assembled to *Creating awareness by adequate knowledge on protection of Intellectual Capital*

CG S Responsibilities of the Board. The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders. [252]

- The experts commented that this is a Duplicate of other sources mentioning the importance of assigning a accountable and responsible person at the Board of Directors level. One expert said "*although I agree that the entire board should take responsibility, not just one man*". The expert panel agreed on the replacement of this practice by more specific practices: *Appoint a responsible and accountable board member for risk management and sees that the company has implemented an effective ongoing process to identify risk, measure its potential impact against a set of assumptions, and then activate what it believes is necessary to proactively manage these risks* [256].

During this research step, the experts concluded that Corporate Governance practices are often vaguely phrased and therefore it is difficult to implement them or perhaps not implemented at all because the organisation does not know how. Because of this vague specification of important Governance Practices, I asked the experts to rephrase these practices into a more understandable format. Many of the Corporate Governance practices are a derivative of others so a large number of practices are marked as duplicates. The experts were asked to mark these and they were subsequently deleted with the facilitator agreeing. All of the experts pointed out that many of the governance practices they assessed are crucial to the final implementation of good Security management practices into operations. They are pre-requisites for any organisation.

RG P Aligning risk appetite and strategy. Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks [258].

-One of the experts commented that this should be formulated more simply; risk appetite should be aligned with business strategy and accompanying objectives. Determining the organisations risk appetite is stated in most of the Governance academic and practice-oriented sources, mainly because history taught us the importance of doing so (see for example cases like Enron, MCI Worldcom, etc.).

RG RM BoD understanding of risk philosophy and appetite. The board should understand the entity's risk philosophy and concur with entity's risk appetite [259].

- The experts commented that the risk philosophy always needs to be linked to business strategy and therefore risk appetite. It is important to note here that understanding risk philosophy has more to do with the awareness to recognise and understand the risk philosophy at board level and the behaviour and attitude towards risks.

During this step a large amount of consensus was achieved. Most of the experts recognised the most relevant Governance Practices. This is acknowledged by the fact that during this step of the research the lowest level of variety is measured in GSS. This is especially the case with the practices: "*Determine Roles, Accountabilities and Responsibilities*" and "*Transparency*".

Numerous Risk Governance practices again overlap with each other or even other disciplines: for example, Roles and Responsibilities, Stakeholder identification and identifying events that can threaten the business continuity. It is interesting that the leadership of driving Risk Governance practices seem to be important. COSO mentions this numerous times in several reports [259], [258]. Within Corporate Governance practices literature, this subject is never mentioned perhaps because it's assumed that leadership is inherent to the nature of any board member. Nevertheless, according to the literature leadership is one of most contributing factors to business success or failure [20], [265]. In this case it is an essential finding to take into consideration.

In this first step we assessed the Governance practices within the Enterprise Governance of IT domain. Since businesses depend more and more on IT, the security of these systems is greatly important. Not only the confidentiality of the information but also the integrity and availability. This makes the practices from Governance of IT relevant to an examination of Business Information Security Governance. Again, we address the best candidates and the ones that were discussed most intensely;

ITG P IT performance measurement (e.g. IT balanced scorecard) [217]

- The experts commented that this could be aligned with the BSC from business units.

ITG P boards review the risk management approach for the most important IT-related risks on a regular basis, at least annually [18]

- Experts mentioned that these plans could be integrated in the total of risk management (so IT risks should not be separated).

ITG R IT leadership [105]

- Experts pointed to the very high level of this practice. All of them emphasised that leadership is always a very important practice, especially at Governance level. In other words "*Lead by good example*".

During this step of the research, the experts find full consensus that the IT Governance practices mentioned above are less relevant to the security topic. The main reason for this is that there is a huge overlap with the other practices. IT is part of the organisation but less integrated than for example risk management (risks arise on multi-levels, personnel, finance, safety, etc.). Another argument is that IT Governance practices can be incorporated by rephrasing them into Information Security Governance Practices. In other words, we use the relevant practices from this step and incorporate them into the next step: assessing and organising the Information Security Governance Practices.

Finally, organising Information Security Governance (ISG) Practices was on the agenda of the experts' panel session. This practice appears to be the most closely related the topic of Business Information Security Governance. Therefore, it potentially hides the best candidates. The next important step is have experts assess all of them and make comments if they disagree. An important consideration for me was that Information Security Governance is not the same as Business Information Security Governance. Incorporating the security of the business - and all its related dimensions e.g. risk management- as a whole is of the essence in the exact distinction and specification of this domain. The hypothesis that most of the relevant practices for BISG might potentially lie in other disciplines than IT and Security can be told by the score of the practices. If only ISG practices arise in the ranking, the hypothesis is false. If other Governance disciplines arise, the hypotheses are confirmed.

Acknowledging all relevant Governance practices in selecting the core BISG practices is important. Especially because all previous research and literature address the necessity of Security management and do not address Governance. Governance is a necessity for mandating security management. Hence, "Good Governance" is essential to mandating it into the efficient operationalising of security management. An assessment of the ISG practices provides the following findings:

ISG RM IT Dependency. Understanding the critical nature of information and information security to the organisation. [261]

- Experts comment that this practice is vague. "What to understand, and especially, how to measure understanding? And by whom?" The experts also mentioned that this practice is relevant since some of the BoD members are not aware how much their business relies on IT.

ISG RM Security awareness at level of board of directors. A certain level of awareness about business risks, business critical information, level of information (IT) dependency, kind of threats from outside and inside. [217]

- Experts completely agreed on this practice since organisations nowadays do not have adequate knowledge or the awareness to enforce appropriate action.

Experts agreed that practices ought to be simple and easy to understand by board members.

Examples are;

ISG P *Do simple risk assessments*. Do simple, subjective risk assessments, and put your effort into improving security [261].

ISG P *Report simple* (Red-Yellow-Green). Use a simple High-Moderate-Low (Red-Yellow-Green) ranking [261].

ISG RM Create a measurable security-aware culture [262].

ISG P *Security maturity assessments*. Determine current BIS maturity level based on COBIT [22].

In conclusion, we can state that, at the end of this step (analysis of and completing practices per domain), the expert panel team derived a 'clean' list of practices from a large amount of data in the literature. Some of the practices were deleted (duplicates) and some were rephrased to avoid misinterpretation in the next research step, ranking the practices on effectiveness.

5.3.4 RANKING THE GSS DATA

The level of effectiveness is the first selection method. A Likert scale was used on which 0 ranks as not effective and 5 ranks as highly effective, mainly because it is our intention to select the best working practices according to experts. In this way this research project can contribute to solving the problem of the low level of security within organisations. These best working practices can later be used as candidates for the next ranking on "Ease of Design and Realisation", "Ease of Maintenance" and "Ease of Implementation", also on a scale from 0 to 5. Assessing and ranking all practices over these three dimensions will enable us to determine which practices will work on a management level according to the principles of ISO 38500 standard, and can be monitored and evaluated by the Board (Governance level). In consensus with the experts I decided to rank the top practices, measured from 4 and above on effectiveness. In order to compile a list to be judged on these four criteria (1. "Effectiveness", 2. "Ease of Design and Realisation", 3. Ease of maintenance and 4. Ease of Implementation) that contributes to the ongoing process according to the ISO 38500 principles. The graph in Figure 32 reflects the outcomes of this research phase. It displays the accumulated score on Effectiveness, Ease of Design & Realisation, Implementation and Maintenance. This ranking also provides insight into the level of theoretical practices ranked via GSS for practical use. These views of the practitioners on the practical usefulness of the theory in question provide the latter with necessary and meaningful feedback.

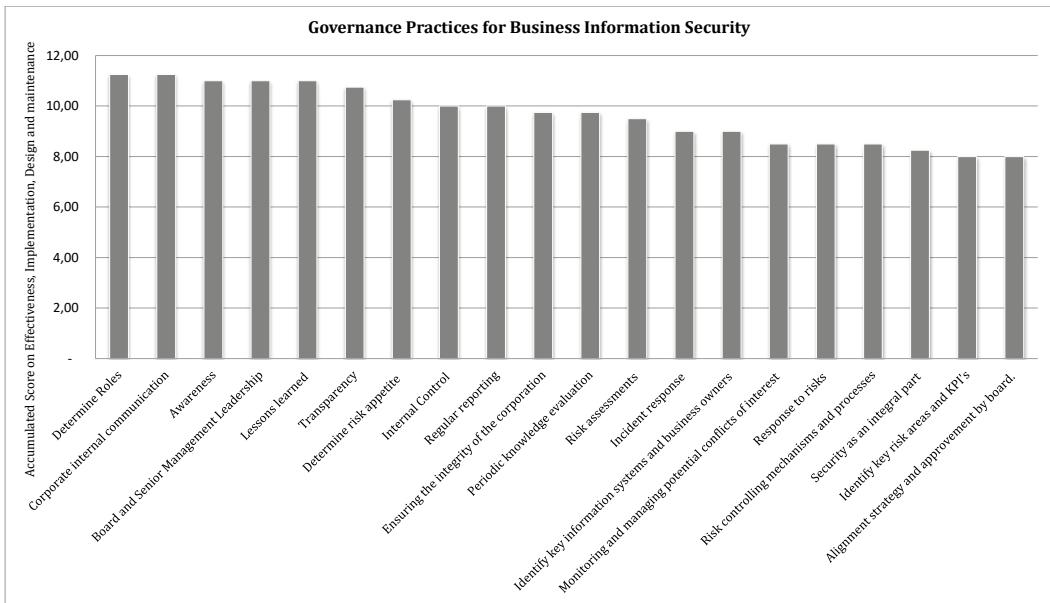


Figure 32: Top 20 Practices for BISG according to the Literature and Experts Validation.

5.3.5 FRAMEWORK FOR BISG PRACTICES

The research question formulated at the beginning of this project - "What is a framework for Business Information Security Governance practices, according to the academic literature on the subject and the views of experts?" - can now be answered in a dual way. Firstly, the framework for Business Information Security Governance consists of all the relevant literature on the topic, which has been examined and elaborated on throughout this section of the thesis. Secondly, this framework consists of three components: structures, processes and relational mechanisms. With the help of the expert panel research, through GSS team collaboration, the researchers organised, ranked and captured the most relevant and effective ones, per component in the theoretical framework visualised in Figure 33. This framework can serve as a theoretical departure for further research on the basis of the following important questions:

Which factors influence the acceptance of Governance practices in an organisation? These factors include budgets, knowledge, innovation, culture, demographics and so on.

Do these practices address the major business risks inherent to the current security problems?

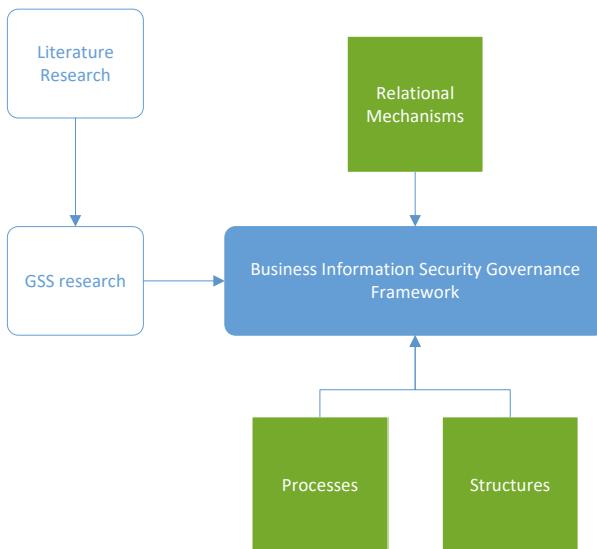


Figure 33: Framework for BISG research

5.4 CONCLUSIONS

This research contributed in the delivery of a set of practices that contribute the conceptual framework for BIS. The final result of this research part is reflected in a top 20 Business Information Security Governance (BISG) practices. The top 10 is listed in Table 9. And the entire data set can be accessed via <https://easy.dans.knaw.nl/ui/datasets/id/easy-dataset:77502>

The use of GSS enables the researcher to objectively examine practices by making use of an objectivism is a safeguard to avoid the personal bias of the researcher, as referred to in Chapter 2. The hypothesis that other Governance practices than IT and Security would deliver relevant practices for BISG has been confirmed. Half (50%) of the top twenty Governance practices for Business Information Security come from either Corporate Governance or Risk Governance. As a result of our findings, a highly significant core set of Business Information Security Governance and Executive Management practices could be established. In the next phase of this research project, this core set must be tailor-made for specific (organisational) environments by:

1. Analysing the influencing factors mentioned in the framework section;
2. Testing the acceptance on the part of the executive management of organisations;
3. Investigating whether these practices can be evaluated, directed and monitored, according to ISO38500 Governance within the organisation.

In this further research, the researchers present the core set and the influencing factors (i.e. large data sets) to an organisation, to small groups of BoD and MT's within this organisation. And ask them to participate in the collaboration process as to what works for them and how organisations organise and measure their state per top practice (e.g. roles, risk appetite, incident response) and formulate follow-up actions (monitor, evaluate, direct) in order to maintain a certain level of Business Information Security maturity. This practice-oriented research will contribute to organisations since the latter can adopt the core set of governance practices. In this way a socially justified method (due to team collaboration on a large set of predefined data (i.e. top 20)) of practical Business Information Security consultancy will "*encompass social and adaptable security methods that are rigorously developed along with practice*" [151]. The result of this research is the design of a conceptual framework to monitor, evaluate and direct business information security governance. According to Hevner's design science research method [138], the next phase will consist of the implementation of the framework in the design artefact.

Table 9: Top 10 Business Information Security Governance practices in detail.

#	TOP 10 BISG PRACTICES	SCORE	LEVEL	SPRM
1	Determine Roles. Accountability and responsibility for Business Information Security at Board and Executive management level. Including the role of the stakeholders.	11.25	Governance	Structure
2	Corporate internal communication on cyber downside. e.g. cybercrime, fraud, theft, forgery, piracy, bullying. Internal communication channels such as intranet. HRM letters. Workshops can be used to educate employees.	11.25	Management	Relational Mechanism
3	Awareness at level of Boards of Directors. A certain level of awareness about business risks. Business critical information. Level of information (IT) dependency. Kinds of threats from outside and inside.	11.00	Management	Relational Mechanism
4	Board and Senior Management Leadership. Lead by good example. Clean desk policy. Limited personal web exposure (personal blogging, video). Software piracy. Shred confidential papers, etc.	11.00	Governance	Relational Mechanism
5	Lessons learned. Sessions after security incidents. Document and report incidents that occur. Also what kind of response to the stakeholders was made and how such an event can be prevented. Take these in consideration for the formulation of strategy.	11.00	Governance	Process
6	Transparency. The company should also consider the need for a confidential reporting process (whistle-blowing) covering fraud and other risks.	10.75	Governance	Process
7	Determine risk appetite. The level of risk and exposure a company is willing to take when it comes to Information Security Risks. To justify decision-making on investments/insurance.	10.25	Governance	Process
8	Internal control. Regularly review processes and procedures to ensure the effectiveness of its internal systems of control. so that its decision-making capability and the accuracy of its reporting and financial results are maintained at a high level at all times.	10.00	Management	Process
9	Regular reporting on security adequacy and effectiveness. Requiring regular reports from management on the programme's adequacy and effectiveness.	10.00	Management	Process
10	Ensuring the integrity of the corporation. Accounting and financial reporting systems. Including independent audits. Ensure that appropriate systems of control are in place. In particular, systems for risk management, financial and operational control and compliance with the law and relevant standards.	9.75	Management	Process

6

DESIGNING AND DEVELOPING THE ARTEFACT

"There cannot be a greater mistake than that of looking superciliously on practical applications of science. The life and soul of science is its practical application..."

-Lord Kelvin in Electrical Units of Measurement", May 3, 1883

This chapter deals with the design and development of an MBIS artefact within a Design Science Research Framework. There are five cases of practical problems that led to artefact requirements that were adopted in building the artefact, these are described in Chapter 7. A case study, investigates an instance of a phenomenon in depth [73]. All five cases have gone through the entire Design Science Research (DSR) cycle as proposed in chapter 2. Thus in this chapter we first explicate the problem before we can set the requirement for the artefact.

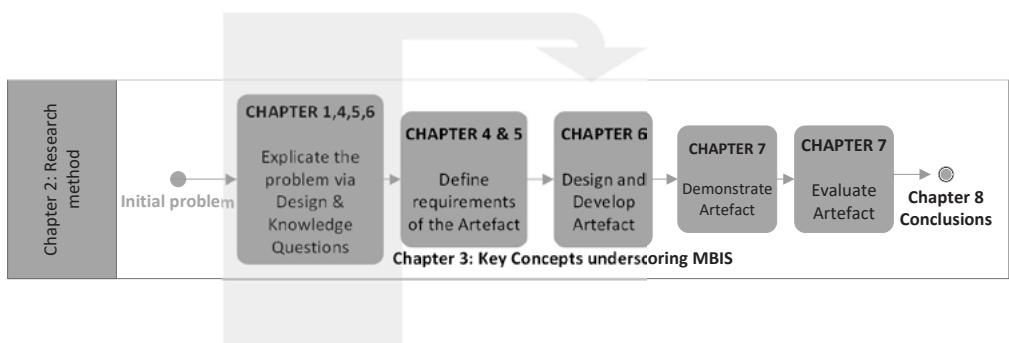


Figure 34: Explicating the problem for the design of the artefact based on Johannesson and Perjons [73]

6.1 INTRODUCTION

Solving numerous practical problems via a Design Science approach requires a) a designed artefact that improves something for stakeholders and b) empirically investigating the performance and effect of an artefact in its context. Within Design Science the design cycle is used to address design problems, via design questions, of the artefact and the empirical cycle is assigned to knowledge questions to gain insights in improvements. In this section the use of numerous DSR methods in order to design and develop the artefact requirements is addressed. This is demonstrated via five DS research projects in recent years (2010-2015) within the Business Information Security domain. All projects were under supervision of Antwerp University and my co-promotors. Some cases have been reported in peer-reviewed published work.

1. The first case involves examining the core functionalities of the MBIS artefact in relation to the target group (which operates in a business environment). The main research question was: *Which management information would CIOs and CISOs consider to be of*

importance when managing their business security (from governance to operation)? In this case we used customer opinions through GSS research. This request provided input for establishing the functional requirements for the artefact. The participants in this case were CIOs and CISOs from mid-market organisations and the research was done in Q4 of 2012.

2. The second case involves exploring and predefining governance practices for Business Information Security, using expert opinion acquired via GSS. The main research question was: *Which governance practices and critical success factors do boardroom members require in their daily management that can help them direct, monitor and control the governance of BIS?* The outcome of that research also formed a set of artefact requirements. This research was performed in Q1 of 2012. We demonstrated the design and development of the requirements.
3. The third case involves exploring and setting requirements for a core set of management interventions which organisations need to take into account in order to increase the maturity level of BIS. The main research question was: *Which core interventions do managers find effective in enhancing BIS maturity level?* In this case we made use of expert panel opinions (through GSS research) to generate and select a core set of interventions that can form requirements for the MBIS artefact. This research was performed in Q1 of 2010.
4. The forth case involved demonstrating how Delphi Research can contribute to generating metric requirements for an artefact. The main research question was: *Which metrics are effective for governance, management and operation in order to measure the MBIS process?* In this case we zoomed into specific knowledge items on metrics that organisations can consider when measuring the maturity level via the artefact. This research was performed using Delphi research in Q1 of 2013 among 40 security managers.
5. The fifth case was used to demonstrate which new knowledge items should be included in the design and development of the artefact in order to better cope with new contextual influences. The main research question was: *What external forces of influence do security managers recognise and how do they cope with them in BIS strategy formulation?* We used experts' opinions via Delphi research to generate new knowledge items. This research was performed in Q1 of 2013.

6.2 EXPLICATING THE PROBLEM TO DEFINE REQUIREMENTS FOR THE DESIGN

The initial activity of DSR is to make the problem explicit (explain the problem). This is the initial phase in the process of defining artefact requirements, as shown in Figure 35. The objective of this activity is to address the problem, indicate its magnitude and the need to solve it, so it is mainly about the importance of the problem and exploring causes. It forced me to think about solutions to the problem and preselect functional or non-functional requirements [224]. It addresses the question: "*What is the problem experienced by some stakeholders and why is it important?*" [146].

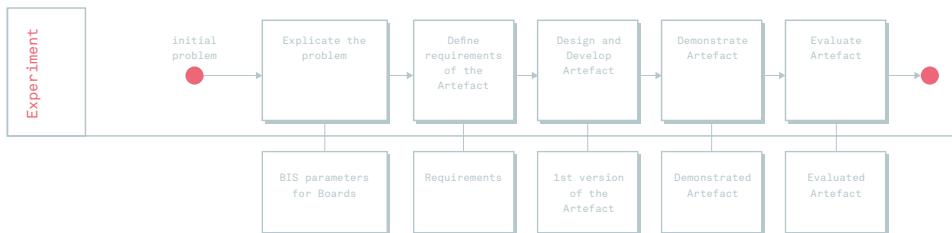


Figure 35: Overview of the DSR framework based on Johannesson and Perjons [73].

Guidelines for 'explicating' the problem are taken into consideration during the examination of the five cases and these are used to structure the research process and thesis sections. Explaining each problem is necessary in order to define requirements for the artefact [73]. And later on to evaluate the artefact.

- 1. Position the problem.** This is important to make the problem that is experienced by some stakeholders explicit and why it is important to investigate. A problem is a gap between the current and the desirable state.
- 2. Formulate the problem precisely.** This is important to gain a mutually accepted view and perception of the problem, the implications and the possible root causes. A problem should be defined precisely so that everybody understands it in the same way. This also helps scope the design science project, making the problem easier to address.
- 3. Justify the problem.** This is important because it should always be positioned in some practice and well justified so that people can agree it is worth addressing.
- 4. Ensure that the problem is of general interest.** It should address a general problem and not just a local practice.
- 5. Ensure that the problem is solvable.** This is important to keep the problem small and thus solvable in a timely manner. Root cause analysis can be performed to identify underlying causes and to pre-synthesise possible solutions to the problem, in order to determine if they are indeed solvable.
- 6. Specify the sources of the problem.** This is important to determine the size and impact of the problem and the fact it is indeed a general problem.
- 7. Describe how the problem has been explained.** This is important to address how the problem is taken into consideration by stakeholders, in the literature and by other interest groups. It can be explained by involving different kinds of stakeholders, such as directors, managers, regulators, employees and customers.

For each of the five cases the initial step, according to the guidelines, is to explain the problem and then – at a later stage – to outline the artefact's functional and non-functional requirements.

6.2.1 EXPLICATING THE PROBLEM PER CASE

6.2.1.1 CASE 1: WHICH DASHBOARD MANAGEMENT INFORMATION WOULD CIO'S AND CISO'S CONSIDER TO BE IMPORTANT WHEN MANAGING THEIR BUSINESS SECURITY (FROM GOVERNANCE TO OPERATION)?

INTRODUCTION

Business managers use business models to operationalise the strategy of the organisation.

The use of management models and methods such as balanced scorecards and key performance indicators are well-known instruments that are used to measure the performance of an organisation. For information security some efforts were made to operationalise the management behind it. The most well-known management instrument is the ISO27001 Information Security Management System and the GASSP²⁵/GAISP and SSE-CMM model. According to Siponen: "*These management systems are generic or universal in scope; consequently they do not pay enough attention to the differences between organisations and the fact that their security requirements are different [3]*". To explain the problem we go into the detail of predefined guidelines:

Guideline	Description
1. Position the problem	Managers lack fact-based BIS management information which influences decision-making. Riabacke (2012) mentioned in his study on decision-making: " <i>the lack of information and precise objective data, that risk and probability estimations made by the managers are often based on inadequate information and intuition,..most decisions are based on intuition and gut feeling</i> " [266] Self-built Excel-based performance sheets lack business priority-related security controls [184] As a result, directors, regulators and other stakeholders currently rely on historical data which is scattered throughout the organisation [9].
2. Formulate the problem precisely	The lack of a centralised fact-based view on BIS (dashboard) limits decision-making and thus poses a liability risk for the organisation and its stakeholders.
3. Justify the problem	Due to these liability risks and the unknown impact on business owners [18] (whether personal or financial), a minimum of management steering information is required [268].
4. Ensure the problem is of general interest	A lack of core BIS management information (facts) and mechanisms to gather data might result in legal, financial and personal implications that are of general interest and are not limited to a department or individual.
5. Ensure the problem is solvable	Provide visibility in a minimum 'set of management information'. This encourages the underlying organisation to provide factual data. The origin of these facts may be databases, log files, scan reports, surveys, processes, reports, observations, checklists, etc.
6. Specify the sources of the problem	The problem has been addressed in the literature and by practitioners [6, 9]. Not only the lack of a dashboard but also the fact that there is often not a process to be monitored at all. Most organisations still practice BIS as a project with ad-hoc interventions [4] and ad-hoc reporting. They lack a consistent working Information Security Management System [3], [61].
7. Describe how the problem has been explained	The BIS topic is multi-dimensional. A <u>director</u> may require a brief summary of BIS facts, for example current state and the route towards a desired state [60], whereas <u>management</u> may want more insight into details. Another perspective is that of the <u>regulator</u> . Regulators require different information in a different format [91]. So multiple stakeholders have multiple demands. In this example we scope the problem of creating a core set of management information. Hence, managers can use this to inform their board.

6.2.1.2 CASE 2: THE LACK OF GOVERNANCE PRACTICES AND CRITICAL SUCCESS FACTORS FOR BUSINESS INFORMATION SECURITY

Theorists and practitioners generally observe good security management practices but also indicate that less attention is paid to governance [239], [18]. This is a problem because security breaches have tremendous implications for the continuity [7], civil or legal liability, reputation, employability and financial position of firms [269], [270]. Most of the security models focus on management and pay less attention to security governance. The lack of dedicated governance practices for Business Information Security is a limitation for today's boards of directors. We explain the problem according to the guideline:

Guideline	Description
1. Position the problem	A board of directors lacks insights into adequate governance practices for BIS and factors of influence (critical success factors). The literature prescribes many corporate governance, risk governance and IT governance practices but there is a lack of Information Security governance practices that have been tested rigorously and validated. This becomes problematic when regulators demand a governance process in order to maintain a licence to operate.
2. Formulate the problem precisely	A lack of insight into governance practices that can function as a core set of principles that contribute to increasing the Security Governance Maturity of organisations.
3. Justify the problem	Due to the increase in cyber threats to organisations it is evident that boards of directors require insight into practices that they can adopt, direct, monitor, control and measure in a continuous manner. Due to the liability risks for the organisation and the unknown impact on board members, a core set of governance practices is required that boards can apply.
4. Ensure the problem is of general interest	Insight into proper governance practices and the accompanying critical success factors is needed in order to stay compliant and to perform good stewardship. If non-compliance is accompanied with failing governance processes, this has broad implications for stakeholders, customers and employees (exceeding the impact of local practices).
5. Ensure the problem is solvable	By providing visibility for a core set of governance practices for BIS the first step in solving the problem is made. Adding a set of critical success factors that board members can apply and act on will further contribute to solving the problem. By continuous use of the list, today's boards also have monitoring capabilities (e.g. parameters of control).
6. Specify the sources of the problem	The source of the problem lies in the embryonic field of BIS. There are numerous best practices at an operational and tactical level, but these are limited at a strategical level. One main cause is that the solution lies not only in instrumentation, but also in softer intangible factors e.g. leadership and culture.
7. Describe how the problem has been explained	This lack of adequate governance practices for BIS is a problem for boards as well as for regulators that want to keep track of the company's performance by evaluating, directing and monitoring BIS. One set of BIS practices involves achieving consensus among stakeholders, provides strategic direction and enables control of the subject.

6.2.1.3 CASE 3: THE LACK OF A CORE SET OF INTERVENTIONS FOR MBIS

In Chapter 4 the problem of “*the absence of a core set of interventions that can be applied to enhance the maturity level of BIS within mid-market organisations*” was explained. This made it unclear for managers what to implement in order to increase security maturity. Managers also experience a knowledge gap in terms of “whether they are doing the right things” [90] (efficiency) and, if they do the right things, “whether they are doing them well” (effectiveness) [64]. This makes it a dual problem. The first problem is the lack of a clear list of interventions that contribute to improving BIS. The second problem is the absence of adequate knowledge to maintain this list of core interventions in a practical environment.

Guideline	Description
1. Position the problem	Managers' lack of a core set of interventions that are effective and easy to implement in order to increase the level of BIS maturity. In the literature this problem is addressed as a management and directors' problem [31]. The problem becomes more complex due to the overwhelming number of frameworks [3], [62] and their complexity [9].
2. Formulate the problem precisely	The absence of a core set of rigorously established interventions for managers leaves them struggling with complex and overwhelming frameworks.
3. Justify 4. the problem	Due to the liability risks towards the organisation and the unknown impact to board members, a minimum set of interventions that an organisation needs to adopt in order to improve the maturity of the BIS position is required.
5. Ensure the problem is of general interest	Small, medium and large companies share the same problems. Big companies are perhaps regulated and therefore more likely to reserve budgets but mid- market companies suffer from insufficient resources, a lack of a sense of urgency and the need for simple tools that fit their limited needs. A lack of core BIS interventions results in legal, financial and personal implications that are of general (stakeholder) interest and are not limited to a department or individual. When the organisation plays a vital role in the economy or infrastructure of a nation it is also a social problem.
6. Ensure the problem is solvable	Gaining insight into a minimum set of BIS interventions and adopting these in business processes will contribute to solving the problem and provide directives for future monitoring.
7. Specify the sources of the problem	The problem has been addressed in the literature by academics and practitioners. Several authors have described BIS as complex and they warn organisations about knowledge gaps [9]. The authors also address the problem of the complex and overwhelming frameworks such as ISO27K [3], which are hard to maintain and monitor [61].
8. Describe how the problem has been explained	The absence of a core set of security maturity interventions has been described in the literature [64]. The problem becomes more visible as companies increasingly trade digitally and suffer financial damage if security is not practised at a certain maturity level [175], [272].

This problem led to a research problem that was answered via Group Support System (GSS) expert panel research and an extra validation by responsible managers in mid-market companies. This step was done to increase the validity of the construct that was to be established at the next stage. The final result is a set of interventions which mid-market organisations can use and they can also function as requirements for the design and development of the artefact.

6.2.1.4 CASE 4: THE LACK OF EFFECTIVE METRICS AT THE GOVERNANCE, MANAGEMENT AND OPERATIONAL LEVEL IN ORDER TO MEASURE THE BIS PROCESS

Practitioners have developed numerous BIS metrics for organisations, for example NIST [273] and ISACA [208]. Pironti [274] stated; "*Information security is an ever-changing and evolving activity. To have accurate visibility to these changes, an organisation must establish, maintain, monitor, interpret and report effective metrics and measures. The threats that an organisation's information infrastructure faces, along with the controls and capabilities that must be deployed to counteract these threats, are constantly changing and evolving. This requires the measures and metrics that are employed to monitor the performance of Information Security governance to be adaptable and flexible to be a positive and valuable asset to the organisation*" [274]. With this, Pironti [274] emphasises the need for clear metrics that boards of directors can understand and monitor. ISACA developed, in COBIT5 for Information Security, a set of metrics per COBIT domain [56]. This resulted in a huge number of metric candidates that can be selected and implemented, from the governance down to the operational level. Jaquith [275] developed metrics for operational, technical and security programmes. Limited academic research has been done on developing metrics for the governance of Business Information Security.

Guideline	Description
10. Position the problem	Boards of directors lack clear predefined metrics to direct, monitor and control BIS governance. The knowledge that is required for developing and maintaining these metrics requires continuous effort. This makes measuring and controlling BIS problematic.
11. Formulate the problem precisely	Without measuring criteria and instruments BIS becomes hard to direct, monitor and control. Because it is not yet known what is good or bad. There is no empirical evidence compared to for example the automotive or aviation industry. This also applies to external stakeholders who need to judge if adequate management is done, based on predefined metrics or KPIs.
12. Justify the problem	Due to the liability risks for the organisation and the unknown impact on board members, key metrics for measuring and managing – as well as the knowledge needed to maintain these items – are required.
13. Ensure the problem is of general interest	A lack of metrics limits the board/manager in doing his or her job, taking or delegating responsibility and ensuring accountability. The implications of having limited or no steering information results in legal, financial and/or personal implications which are of general stakeholder interest and therefore not limited to a department or individual.
14. Ensure the problem is solvable	Having knowledge and insight into metrics that are relevant can contribute to solving the problem.
15. Specify the sources of the problem	The source of the problem is dual. First there is the required knowledge about which relevant metrics to consider, implement and maintain. Then there is a need for insight into which types of metrics are useful for a specific organisation.
16. Describe how the problem has been explained	Numerous management authors describe the necessity of management instruments and KPIs to successfully steer a company [268], [47]. Limited research has been done on metrics relevant for BIS [174] and how to acquire and develop reliable knowledge about BIS measurement models and metrics.

6.2.1.5 CASE 5: A LACK OF KNOWLEDGE ABOUT STRATEGIC EXTERNAL FORCES OF INFLUENCE THAT ARE RELEVANT TO BIS STRATEGY FORMULATION

The risk of exposure after an incident, as well as the financial implications should be enough for most organisations to reconsider their business information security strategy. The economic impact of breaches on organisations has been studied. Ishiguro et al. [50]. Cashell et al. [47] studied movements in the stock price in the aftermath of an information security breach or after a privacy incident [276]. All of these studies confirm the need for a dedicated security strategy. But designing and implementing a security is a challenging task to master, especially when certain knowledge is not available. Pai states [67], in his study, that sharing knowledge at a very early stage is necessary. Michael Porter states that knowledge sharing about influential forces is of the essence in order to determine which battle to choose. Michael Porter's five forces model is an example of a management instrument which can assist business leaders in making strategic plans and reveal knowledge on why certain forces must be controlled and others need not. Initiating the right forces that are relevant during execution is essential. Porter states: "*A perfectly executed but mediocre strategy won't really help the organisation*" [277]. To get an understanding of strategic knowledge items we consider using proven methods or models for strategising and re-using these in BIS. First we articulate the problem of the absence of strategic knowledge items and, at a later stage we determine the requirements of the artefact.

Guideline	Description
Position the problem	The BIS domain is dynamic and complex [9] and cyber threats are evolving at a rapid pace. This makes it difficult for managers to predict certain strategic evolutions. Nevertheless it is up to these managers to protect the organisation against unforeseen surprises. So they rely on those living in a 'system world' [278] to articulate 'mystic' technological language. We can compare this with the domain of competitive analysis for strategy formulation. It is hard to predict tomorrow's competitors but modelling the competitive field into groups helps structuring and doing analysis [216]. A good example is the five forces model of Harvard professor Michael Porter. When we compare this to the BIS domain, we need additional knowledge on strategising the future influences of the company and help in predicting and advising the board on strategic directions.
Formulate the problem precisely	A lack of adequate knowledge and existing management models to continuously advise boards of directors on strategic choices in the BIS domain*.
Justify the problem	Strategising the future of the company is self-evident. Formulating and implementing a security strategy is important but rarely done [111], [265].
Ensure the problem is of general interest	When organisations do not take BIS into consideration in their strategy this can have numerous implications. On the reputational side due to a loss of trust, on the continuity side and on the perceived value of the company [51], [50]. This can sometimes result in bankruptcy [43], so it has become a socio-economic problem of general interest.
Ensure the problem is solvable	The use of existing management models about strategy, to be used by security practitioners, will contribute to solving the knowledge issue. Boards of directors can help security practitioners gain insight into their management models and shed new light on solving new problems with proven methods and models.
Specify the sources of the problem	More impact can be made on boards by using existing models from the world of business [278], focusing on risks that are recognised in this world and articulated in its language.
Describe how the problem has been explained	Knowledge about the strategy of the company lies with the board, while knowledge about the security of systems lies with security experts [278]. A lack of knowledge exchange between these groups is limiting the success of security adoption by boards of directors [9]. Understanding both worlds would contribute to solving this problem [279].

*At the Infosec Dialogue in London (UK) on 4 October 2015 I polled 30 CISOs on their acquaintance with Michael Porter's five forces model. None were familiar with the model. Video recorded on 4 October 2015.

6.2.2 FIVE CASES OF DSR REQUIREMENTS FOR THE DESIGN AND DEVELOPMENT

Now that we have articulated five cases of business problems, we can start defining the artefact requirements accordingly. This step addresses the question: *What artefact can provide a solution to the explained problem and which requirements for this artefact are important for which stakeholders?* First we examine the articulated questions more in detail to set specific requirements for the artefact. The function of a requirement is to show what the artefact can do in solving a predefined problem for a stakeholder. The function is translated into requirements and these functional requirements become the structural requirements of the artefact. This structure represents the internal working of the artefact, the components it is built of and how they interrelate with each other. Another aspect is the definition of non-functional requirements. Those requirements are not functional and can be structural or environmental in nature (context). The context is the external surroundings and the conditions in which the artefact will operate. The effects of the artefact are the way in which the artefact will change the context. Effects can be divided into *intended effects* and *side effects*. In this chapter we elaborate, based on the five cases of practical problems, the research methods used in order to examine the problem and to derive solutions. The primary objective is to distil potential artefact requirements that can contribute to solving the problem. To move from a problem definition towards requirements definitions and include the contribution to the stakeholder, Wieringa's method [143] is applied. Wieringa proposes so-called contribution arguments. These encouraged me to justify the choices involved in setting requirements and a *contribution argument* is thus articulated. This is an argument that satisfies the stakeholders' needs and contributes to a stakeholder goal in the problem context. Jackson (1995) also refers to satisfaction arguments as part of the software engineering problem-solving approach [278]. A contribution argument has the form:

(Artefact requirements) x (Context assumptions) contribute to (Stakeholder goal)

As mentioned in Chapter 2, the applied research strategies and methods are creative, on the one hand to answer knowledge questions, and parallel to that to solve real-life problems that occur in organisations, with the underlying intention to generate new knowledge for the knowledge base. Use is made of creative methods such as surveys, expert groups and action research to gain knowledge about stakeholder's perceptions about a potential solution. So the solution lies in a method which captures and records these requirements. A working method is required that encourages people to critically (re)think when carrying out a certain process. When this representation of an idea, such as a method, becomes concrete or tangible, one can speak of an instantiation.

6.2.2.1 CASE 1: DEFINING KEY MANAGEMENT INFORMATION FOR BIS AS ARTEFACT REQUIREMENTS

BACKGROUND AND INTRODUCTION

We now explore the artefact requirements through the use of a GSS panel discussion with the target group representing the stakeholders that suffer from the problem. The main research question was: *Which management information would CIOs and CISOs consider to be of importance for managing their business security (from governance to operation)?*

RESULTS OF THE GROUP SUPPORT SYSTEMS SESSION

We make use of GSS to elicit views from professionals that advise board members on current and future topics, such as security. GSS facilitates brainstorming, discussion and prioritising and captures per step all relevant data that was referred to by the participants [114], [112]. To set the scene during the GSS session I started with introductory questions. By making use of the Gartner Hype cycle I provided a view on future evolvements in the industry and how they relate to the CIO or CISO profession. To brainstorm and share a common views on trends in IT the participants were asked to discuss innovations for the next five years, and then they were asked to raise any extra relevant innovation besides that provided by the researcher.

The first introductory question was: *Discuss with your partner an innovation – over the next five years – to be included in the session*

This resulted in list of eight items which they were asked to rank, based on their importance to the organisation in terms of business information security.

The second introductory question was: *Rate the importance to your organisation for the next five years from the perspective of business security. Scale: Rate from -5 to +5*

This resulted in a ranked list of innovations for the next five years according to the CIO and/or CISO in relation to BIS.

With this knowledge about future innovations and a certain mind set created during the session, the CIOs and CISOs were asked to raise key management information. They were asked:

Which management information would you consider to be of importance to manage your business security (from governance to operation)?

In the next phase of the research the participants were asked to prioritise the management information items. This resulted in a prioritised list of items (displayed in Table 10.)

Table 10: Case 1: Designing and developing the artefact. Key management information.

ITEM	RATING	ABSTAIN	VARIABILITY
1. <u>Risk thermometer</u>	10	0	0%
2. <u>Policy versus implementation versus checking with numbers</u>	8.8	1	48%
3. <u>Factual figures (for management presentation purposes)</u>	8.8	0	43%
4. Hot items	8.3	1	45%
5. Audits, "traffic light reports" trigger is confidentiality	8	0	61%
6. Technology risk exposure to the company expressed as red-yellow-green	8	0	61%
7. Awareness	7.8	1	51%
8. Number of system intruders	7	1	68%
9. Starting point in a number, to compare and measure	6.8	1	45%
10. Number of unsafe communications	6.8	0	62%
11. Fraud reports	6.5	1	46%
12. Market / environment	5.8	1	71%
13. Image damage	5.5	1	100%
14. Insight into only high risks	5.3	2	46%
15. Work instructions. SMART targets and milestones	5.3	2	10%
16. Policy	5.3	2	10%
17. Tasks, responsibilities and authorities (accountable versus responsible)	5.2	0	74%
18. Stakeholders we are digitally dealing with	4.8	1	67%
19. Spam report	4.8	0	67%
20. Numbers of insecure devices (e.g. login attempts)	4.6	0	67%
21. Number of password resets, number of digital attacks	4.2	0	71%

In the last phase of the GSS session the CIOs and CISOs were asked "what keeps them up at night?" The purpose of this question was to first identify new knowledge items that had not been examined, raised or discussed before and thus check if the session covers most of the knowledge items. Secondly to share knowledge and meanings between the participants and leave room for final discussion that might be of interest in the advancement of this research. An interesting finding raised by one of the participants is a "trashbin check" and "speer phishing the CEO." This is interesting because trashbin checking is something we know from marketing research but not within security. Speer phishing the CEO is an upcoming phenomenon (sometimes referred to as Advanced Persistent Threats), which is relevant for boardroom members to know and how they can protect themselves against this phenomenon.

The session was held in Veenendaal in the Netherlands in Q1 of 2012. The complete report can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

CONTRIBUTION ARGUMENTS

To formulate the contribution argument a decomposition of the problem into requirements is made.

Case 1: Defining key management information for BIS as artefact requirements						
Method	Intended effect	Side effect (knowledge)	Stakeholder Goal	Artefact requirement	Context assumption	Contribution argument
Through GSS the stakeholder group discussed (brainstormed) on numerous items that influence their view on the BIS topic.	New gained knowledge within the group. Exchange of knowledge and viewpoints between the participants.	Take notion of future trends and hypotheses in the IT industry that influence BIS	Gain control over core BIS management information via a prioritised set of items	A prioritised <u>key set of BIS management information</u> criteria that can be used and presented in a <u>dashboard</u> .	More awareness by stakeholders (such as regulators), directors and managers. As well as more insight into the BIS state of the organisation	Provide stakeholders more BIS detailing on implementation of the <u>policy's</u> , high <u>risks</u> and thereby encourage the entire organisation to deliver the underlying <u>facts</u> (evidence)

ARTEFACT REQUIREMENT CANDIDATES

The first three items gained from the group from Table 10 were translated into the contribution argument. Primarily, to solve the main problem of the stakeholder, being the absence of insights into factual data on risks and policy implementations (regulator policies with the objective of complying). This core management information will encourage stakeholders and directors to gain knowledge on BIS in order to increase awareness of the topic. These three items, facts, risks and policy are set as requirements for the artefact. We frame these three core functionalities as "**Key BIS management information.**" Obviously more functionalities besides the top three were discussed. Since I intend to justify the further process of establishing the artefact in the next phase, just these three items are promoted as candidates.

6.2.2.2 CASE 2: DEFINING BISG ARTEFACT REQUIREMENTS

This section focusses on establishing artefact requirements. The data used in this case is the same as chapter 5. In chapter 5 the focus is to examine relevant Governance practices based upon the proposed method of literature research and GSS, in this chapter the same data is used to design the artefact requirements.

This section was published at the International Conference on Computational Intelligence and Communication Networks in 2015, in Dehradun, India, pages 1097-1104 under the title: *Governance Practices and Critical Success factors suitable for Business Information Security*. The complete publication can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

BACKGROUND AND INTRODUCTION

The second problem articulated in the previous section is the “absence of adequate governance practices for BIS for boards” and insight into factors of influence (critical success factors). The objective of this section is to define artefact requirements that contribute to potentially solving this problem through the use of a DSR artefact. In order to set requirements for the design, artefact “requirement design questions” are formulated in the text below.

The absence of governance practices relates to the low level of awareness of security issues on the part of businesses [27], [78]. Theorists and practitioners generally observe relative proper security management [280] practices but also indicate that less attention is paid to governance practices [281], [210], [282]. This is a problem because security breaches have tremendous implications for the continuity [43], civil or legal liability [283], reputation [49], employability and financial position of firms [48], [51]. Hence, it could be argued that information security and its implications no longer only affect the IT department but also several other disciplines.

Research from Ponemon institute has shown that the number of security incidents has increased over the years, as has the financial impact per data breach [11]. In 2009, 25% of EU organisations experienced a data breach (with 47% of Finnish organisations in the leading position). As a result, the European economy has suffered an annual multi-billion euro loss in (source: Europol). The main causes of security incidents are the multiplication of data (Big Data), social media interaction [15], and the increase in cybercrime activities [284], [17].

Chapter 4 revealed that 39% of the examined organisations scored an average security maturity of 2 out of 5. Empirical (measurements) research performed over 2012 and 2013 within 27 organisations confirmed that companies mainly focus on operational security (e.g. firewalling, anti-virus technologies) and less on governance (e.g. compliance, policies, business continuity management). Thus, judging from these studies, there has been a decrease in information security maturity over the last three years, mainly because the current frameworks are “complex and generic”, as Siponen and Willison [3] argued in their research publication. Most of the security maturity measurement models focus on management and only pay attention to security governance in quite a limited way. For example, governance is represented in only 2 domains in the ISO27001 framework, namely ‘Security policy’, i.e. the guidelines in which those concerned with information security need to direct, monitor and report. Compliance refers to the regulations the organisation needs to be compliant with in order to keep their ‘licence to operate’.

The absence of clear practices that can be adopted by boards is a limitation for organisations and for the MBIS process. This research aims first to remedy this by investigating, ordering and ranking relevant practices. And second to define requirements to be adopted in the

artefact. This research is the same research as that described in Chapter 5, only the objective here is to distil artefact requirements, as the aim in Chapter 5 was to elaborate the use of GSS as a research method.

The low level of security maturity and the absence of clear governance practices bring us to the problem statement of this research, namely: There is a lack of insight into governance practices that can successfully function as a core set of principles i.e. requirements in an artefact that can potentially contribute to increasing the Security governance Maturity of organisations.

I intend to contribute to academic rigour and practical relevance by examining governance and executive management practices that contemporary Boards of Directors (BoD) can take into account. The Board sets the direction, monitors and evaluates the effects of this direction (Direct-Control Cycle), when it comes to governing the continuous process of securing and assuring the critical assets of organisations. The international body of Information Systems Audit and Control Association (ISACA) COBIT5 Framework makes a clear distinction: *"governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision-making; and monitoring performance, compliance and progress against agreed-on direction and objectives (EDM)."*

"Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM)."

Basie and Rossouw Von Solms [52] define Information Security governance (ISG) as follows: "ISG consists of the management commitment and leadership, organisational structures, user awareness and commitment, policies, procedures, technologies and compliancy enforcements mechanisms, all working together to ensure that the Confidentiality, Integrity and Availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc.) are maintained at all times." These authors also differentiate between information security, management and governance, and define information security management as: "Management must ensure that the policies and procedures are in place and the operational environment is managed and running smoothly on a day-to-day basis." In the practical field, organisations have become more successful in implementing security management but are still struggling with the implementation of Information Security governance [250], [239]. The scope definition in this research is governance. This means that all the directive-setting and controlling (including monitoring and evaluating) activities are seen as governance [71]. All activities to translate these activities into decisions are seen as management and thus beyond the scope of this research. This is also valid for operational practices. In this research we follow Van Solms' distinction between governance and management [239]. Furthermore, we specifically distinguish between executive management activities and senior and middle management activities. For semantics we use the collective term governance (by which we also mean executive management).

DEFINING THE REQUIREMENT DESIGN QUESTIONS:

The research question underlying this research part is: "*Which practices at the level of governance are relevant for Business Information Security Maturity?*"

To determine which governance and executive management practices are described in the literature, a thorough investigation of all relevant literature in the field was carried out (academic as well as practitioner-oriented literature). Numerous IT governance studies [105], [241], [260] propose process-oriented practices, structure-oriented practices and culturally oriented practices to implement IT governance in practical environments. They do not rely on individual interventions, for example the right structure of the Chief Information Security Officer (CISO) reporting to the CEO. Nor do they emphasise the right culture of awareness at the top to protect intellectual properties. Essentially, the synthesis of the right set of Structures, Processes and Relational Mechanisms (SPRM) delivers a powerful whole [285], [216] and potentially contributes to better governance of BIS. To determine the potential SPrM-based candidate practices for this right set, research question one is formulated as:

RQ1: *Which governance practices in the literature are relevant for Business Information Security governance (BISG)?*

Investigating and structuring the current literature on potential practice candidates for BISG contributes to the academic rigour of security. A thorough validation by experts enables the practical relevance of the BISG practice candidates. This brings us to the second research question:

RQ2: *How do experts validate and rank the Business Information Security governance practices derived from the literature from numerous perspectives?*

An additional design question is raised: *Which BISG practices can be designed and engineered in the artefact?*

RESEARCH APPROACH FOR EXAMINING AND VALIDATING BISG PRACTICES FOR THE DESIGN OF THE ARTEFACT

LITERATURE REVIEW

Little research has been done in the field of governance for information security. Most of the work is based on practitioner-based sources [286], [286], [11]. Thorough academically based literature research was used to answer RQ1. Golden-Biddle and Lock [287] distinguish important steps in reviewing and presenting literature research work.

Initially *Constructing intertextual coherence* – existing knowledge represented and organised in the literature – is needed to denote the contribution of practice in another discipline to the BIS domain. I.e. is a governance practice from a certain discipline applicable in another domain. In order to construct intertextual coherence, a technique that is used is: *Non-coherence*: recognition of many contributions being made in a certain domain but where there is considerable disagreement among practitioners. In this BIS domain there seems to be disagreement on the governance practices needed to be implemented but in fact this is not done, as is shown by the graph (figure 1) in the introduction showing the low maturity level of governance-related domains. There seems to be non-coherence between theory and practice and this leaves room for a contribution to be made. A research aim was to investigate the existing literature on governance practices in terms of *Inadequacy*: items that have been overlooked, or ways of looking at it that can improve understanding, and alternative perspectives or frameworks that can contribute to the current body of knowledge of BIS. The key point of Golden-Biddle and Locke is to achieve a number of things: a) to develop a new version of the literature in such a way that it contributes to the body of knowledge, and to present new insights that could be used to solve a practical problem, and b) The gap or problem in the literature that is identified leads to the research question.

The methodology of the literature review, as proposed in chapter 2, aimed at exhaustively investigating relevant literature for several years (2009-2012) and to create a structured list of these literature sources and derive relevant practices. The methodology used is presented by Bruce in 1994 [288] and it comprises the following steps as proposed by Brymann and Bell in their Book Business Research Methods [74]:

- *List*: A list of comprising pertinent items representing the literature of the subject is compiled from relevant disciplines and multiple sources (academic and practitioner-oriented) [74]:
- *Search*: Identify relevant information. From various disciplines: Corporate governance (CG), Risk governance (RG), Enterprise Governance of IT (ITG), Information Security governance (ISG). These related disciplines are specified in previous research work from Professor Von Solms [52] in 2009 and were used as a point of departure for this literature review. During this stage it was important to identify relevant criteria for the further research phases: a) is the practice identified as a governance practice or as an executive management practice? b) are the practices identified as process, structural or relational mechanism practices? See below for further detailing.
- *Survey*: A critical survey of past and present writing by respected researchers, institutions, committees and authorities. Evaluating the relevance of the literature, considering numerous questions such as How recent is the practice/source? Is it likely to have been superseded? Is the source relevant for inclusion (i.e. governance or executive management-oriented and applicable for BIS)? And evaluating the value of the literature. Does the item (practice) appear to be biased? Is the source acknowledged as an international standard/institution? Does the item provide guidance for future research?

- *Vehicle*: Because of the dynamics of the subject and the international orientation of most practices the literature review functions as a knowledge vehicle. During the literature research years, new insights emerged that helped me gain additional knowledge and viewpoints. This enabled the completeness of the literature review. Investigating more in-depth important citations in the literature helped ensure an exhaustive list of relevant literature and thus enabled the completeness.
- *Facilitator*: The literature review facilitated new insights into the phenomena. It helped sharpen the methodology and next research phases (i.e. input for the next (GSS) research phase).
- *Report*: The focus was on identifying and framing practices in the literature that can provide a contribution to the embryonic field of BIS, thus framing a point of departure for further research. In this case validating the literature research and enriching it with a practitioner's view.

Figure 36 shows how 228 practices from numerous literature sources were marked with relevant criteria according to Bruce. This is relevant to trail back the source, author, origin, etc. at a later stage. The criteria were:

Discipline: The business discipline that the practice is related to

Dimension: Whether a practice is a structure, process or relational mechanism (see next section)

The name: The term used for the practice

Summary/explanation: The description the intention and objective of the practice

Source: The original source of the practice

Date of extraction: The date and time it was extracted

Data source: The digital source from which the practice is extracted.

The entire literature research dataset can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

STRUCTURES, PROCESSES AND RELATIONAL MECHANISMS AS A METHOD FOR MARKING THE DATA IN THE LITERATURE

Earlier research by Van Grembergen & De Haes [187] and Luftman [186] served as a starting point for aligning business goals to governance practices. De Haes & Van Grembergen [108], [217] suggest deploying a collective set of structures, processes and relational mechanisms (SPRM, e.g. culture and knowledge) in order to successfully implement IT governance in organisations. In this research we propose the same methodology to mark the data in the literature and subsequently distil a core set of practices and CSFs that can be used by practitioners. This theory was successfully applied in previous studies and led to effective and practical methods such as COBIT [208].

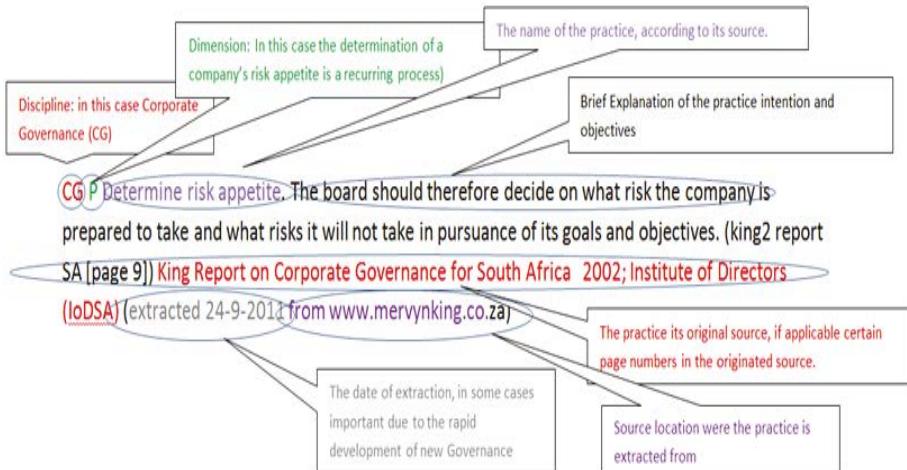


Figure 36: Sample of marking governance practices during the literature research.

In this research we used this SPRM methodology to mark the data in the literature, and later on distilled a core set of practices that can be used by practitioners. These also formed requirement candidates for the artefact.

Such work as exists is based on practitioners [286], [280], [78], [281]. We propose to add another layer to this type of research by also examining academic literature in order to answer RQ1. The methodology of the literature review was to exhaustively investigate relevant literature over several years (2009-2012) and to list items in a structured way using the methodology proposed by Bruce in 1994 [288]. Other disciplines closely related to BISG were investigated. These were Corporate Governance (CG), Risk Governance (RG), Information Security governance (ISG) and Information Technology Governance (ITG).

RIGOUR AND RELEVANCE

Most of the current rigour in the security domain is prescriptive in nature. To acquire a more profound understanding of the gap between what needs to be done to ensure academic rigour and what is prioritised by practitioners (relevance) validation of the collected list by practitioners is required. Firstly, we needed to know which practices are lacking in the literature and whether this might cause a low level of governance maturity. Secondly, in order to get the practices adopted by Boards of Directors an expert panel research is proposed. Finally, it is our aim to answer RQ2: "How do experts validate and rank the Business Information Security governance practices derived from the literature from multiple perspectives?"

The experts were requested to supplement, improve and test the earlier collected practices from multiple perspectives (relevance criteria, i.e. effect, ease of design, implementation, and maintenance) and rank them in order to achieve a certain sequence in the application of the practices. Figure 37 displays the research process flow used to find answers to the research questions.

GSS EXPERT PANEL RESEARCH FOR DEFINING THE BISG PRACTICES

After collecting all the data in the literature, expert views were needed to enrich, assess and evaluate the identified practices in more detail, using a Group Support System (GSS). Expert groups make it possible to elicit views and perceptions from a diverse group of experts [114], [112]. The role of the facilitator is important in order to avoid the "Asch Effect" where certain individuals dominate group dynamics and therefore the outcome of the discussion [117].

Moreover, the number of items (in this case 228 practices) to be discussed is an important variable in the setup of a GSS meeting. Participants discuss comprehensive lists of items and a number of measures are necessary to facilitate this process. To enable experts to remain focused during the meeting a 'carrousel' is introduced in which each expert starts with a different list of items to assess and comment on [129]. The experts were selected according to the following criteria: they have a BA or MA degree in Information Systems, plus industry certificates e.g. Certified Information Security Manager (CISM), Chief Information Security Auditor (CISA), Certified Ethical Hacker (CEH) and Registered EDP Auditor (RE). They have more than 10 years of experience in Business Information Security and they are full-time practitioners. The four experts were perfectly situated to select and rank this huge amount of data in the literature, which makes their assessments highly relevant.

RESEARCH FINDINGS OF THE LITERATURE REVIEW AND EXPERT VALIDATION

Literature mainly refers to governance where it leads to executive management practices (e.g. C-suite level). We started our research by examining all literature on governance and executive management practices relevant to the topic of Business Information Security. These governance and executive management practices and their related sources, according to Von Solms [210], are:

1. Approximately 50 best practices from the **Corporate Governance** discipline were examined. Major sources of origin of these practice: The OECD Principles of Corporate Governance [252]. The Commonwealth Association for Corporate Governance [253]. Internal Control Guidance to Directors, Turnbull Report [254], The Financial Reporting Council (FRC) Combined Code [255]. The King Report on Corporate Governance for South Africa [256]. Bank for International Settlements (BIS) Basel principles for enhancing corporate governance [257]. Security and Exchange Commission add-ons to SoX, Commission on Public Trust and Private Enterprise 2003. All of these can be found in the Corporate Governance Book (Oxford University Press), which covers all international Corporate governance codes [59].

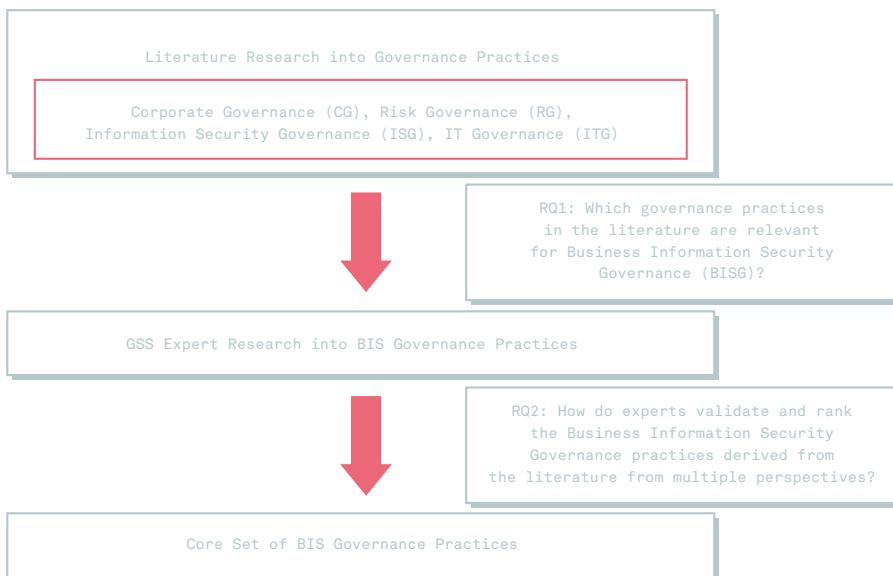


Figure 37: Research process, including research questions for defining BISG practices

2. A major component of practising good governance is the **Risk Governance** discipline. Insufficient Risk governance and management has enormous consequences for all major stakeholders [20]. The judgement and management of IT-related risks has become increasingly important to the success of businesses [197]. For the assessment of all relevant Risk governance practices, I examined literature from: COSO's Enterprise Risk Management Integrated Framework [258], COSO's "Embracing Enterprise Risk Management": Practical Approaches for Getting Started [259], COSO's "Where Boards of Directors currently Stand in executing Their Risk Oversight Responsibilities" [31], King's Report on Corporate Governance for South Africa – 2002 [256], and Douglas Hubbard's study on Risk Management Failures. A total of forty Risk Governance Practices were selected.
3. Forty **IT governance** practices were selected from several sources: IT Governance Institute, "Information Risks: Whose Business Are They?" [18], De Haes & Van Grembergen's "Practices in IT governance and Business/IT Alignment" published in ISACA's journal (Information Systems Audit and Control Association). Weil & Ross' "IT Governance" [260] and De Haes & Van Grembergen's book "Implementing Information Technology Governance; Models Practices and Cases" [217] and Van Grembergen's "Strategies for Information Technology Governance" [108].
4. During the selection of the literature, numerous academic and practice-oriented sources were investigated, mainly to judge their appropriateness for ISG practices. I investigated a large number of resources on **Information Security governance**, because this discipline is the most closely related to (BISG). I investigated resources over a longer time

period (2 years) in an international context to avoid missing out on important worldwide developments; multi-sources (from Research institutes such as IDC and Gartner) and academic journals and books (published by Harvard Business Press, Springer, Wiley among others). I also looked at best practices institutes such as ISACA, ITGI, ISF, SABSA etc., and other communities practising Security Governance. An examination of highly respected and well-established literature sources resulted in 98 practices. The major literature sources are: the 2004 Corporate governance Task Force Report of the National Cyber Security Summit [261] chapters "Information Security governance and Responsibilities of the Board of Directors/Trustees." De Haes & Van Grembergen's "Practices in IT governance and Business/IT Alignment", published in: ISACA's journal in 2008 . Von Solms' "The 10 deadly sins of information security management" [51] and other major relevant sources on the ISG topic [262], [22], [263], [63], [264], [209], [52].

This literature research resulted in a list of 228 practices. In this phase of the study, the focus was on researching BIS relevant practices, not on determining where these practices are operationalised. This was done by the experts.

DISCUSSION AND LIMITATIONS OF THE LITERATURE REVIEW

Many of the practices show overlap even within disciplines. For example, the role of the stakeholder in Corporate governance articulates the same intention of the practice in a different way. The OECD refers to "*The corporate governance framework should recognise the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.*"

Whereas the Commonwealth Association for Corporate Governance refers to: "*identify the corporation's internal and external stakeholders and agree a policy, or policies, determining how the corporation should relate to them (Principle 8)*"

The question arises why so few countries have governance codes for overseeing technology risks. The few countries that have developed sound directives are South Africa [256] and The United States [261]. These countries specifically address technology risks in their practices, mainly because they suffer the most from cyber criminality. At the time of writing, the European Commission has also addressed cyber risks as a "Board responsibility."

I have observed the usability of a tremendous number of Corporate and Risk governance practices applicable in the domain of BIS. Judging from practical experience, basic principles such as determining responsibility and accountability (Turnbull Report, COSO, King Report) and the role of stakeholders [253], [31] are not implemented by many organisations.

A limitation of this literature review is time, since the dynamics of this subject and the constantly changing context (e.g. compliance, politics and technology) greatly influence the accuracy of the literature. Another limitation is globalisation. Many governance practices are not widely published, so this research concentrates on the most dominant and internationally accepted ones. We need to acknowledge that it could be relevant to examine these practices. Language is a limitation as well, mainly because this research has focused on the English language and cites only English governance practices (excluding Asian, Arabic, and Spanish examples for instance).

GSS EXPERT RESEARCH

The initial list of 228 practices was further evaluated by a group of four experts during a four-hour GSS session led by an experienced facilitator. In the first round of this evaluation, the experts were asked to justify the quality (adding, undoubling) of the practices. This took two hours with all experts in one group assessing all the practices together at a rather fast pace. In the next round, the experts were asked to evaluate the practices against some attributes such as perceived effectiveness, ease of design and realisation, ease of maintenance and ease of implementation. This took two hour and the experts were not allowed to exchange their view or score with each other.

During this first research phase of undoubling, the experts concluded that Corporate governance Practices are often vaguely phrased and that it is therefore difficult to implement them. They might not even be implemented at all because the organisation does not know how to do so. Because of this vague specification of important governance Practices, I asked the experts to rephrase them into a more understandable format. Many of the Corporate governance practices are derivatives of others so a large number of practices could be marked as duplicates. The experts were asked to do this marking and these duplicates were subsequently deleted with the facilitator agreeing. All of the experts pointed out that many of the governance practices they assessed are crucial to the final implementation of good security management practices into operations. They are critical success factors for any organisation.

After the assessment of the Corporate governance practices, the experts went on to judge Risk governance and practices within the Enterprise governance of the IT domain.

During the GSS session, the experts unanimously told the GSS facilitator and me that Enterprise Governance of IT practices is less relevant to the security topic. The main reason for this is that there is a huge overlap with the other practices. IT is part of the organisation, but it is less fully integrated than for example risk management (risks arise at multiple levels, such as personnel, finance, safety, etc.). IT governance practices can therefore be incorporated into Information Security governance Practices (for instance by rephrasing them). In other words, we use the relevant practices from this phase and incorporate them into our next phase: assessing and organising the Information Security governance Practices.

The final item on the agenda of the expert panel session was the organisation of Information Security governance (ISG) Practices. These appear to be the most closely related to the topic of Business Information Security Governance. The next important step was having the experts assess all of them and making comments if they disagreed.

An important consideration was that Information Security governance is not the same as Business Information Security Governance. Incorporating the security of the business – and all of its related dimensions e.g. risk management – as a whole is of the essence in the exact distinction and specification of this domain. The assumption that most of the relevant practices for BISG can potentially be found in other disciplines than IT and Security can be seen by the score of the practices.

In conclusion, we can state that, at the end of this phase (analysis of and completing practices per domain), the expert panel team derived a 'clean' list of practices from a large amount of data in the literature. Some of the practices were deleted (duplicates) and some were rephrased to avoid misinterpretation in the next research phase, ranking the practices on effectiveness. The three remaining disciplines of Corporate Governance (CG), Risk Governance (RG) and Information Security governance (ISG) now present respectively 34, 31 and 61 practices. This amounts to a total of 126 'specific' practices of processes, structures and relational mechanisms. This total of 126 practices was used in the next 'ranking' phase.

RANKING THE GOVERNANCE PRACTICES

After the expert panel had compiled a set of practices, it was important to rank them on relevance for an organisation. In order to compile a comprehensive and practical list that can function as principles, I formulated these four ranking criteria as:

1. Effectiveness
2. Ease of Design and Realisation
3. Ease of Maintenance
4. Ease of Implementation.

The result should be a frame of reference of core principles and the level of effectiveness was the first selection method. Ranking practices on effectiveness directly contributes to the potential increase in security maturity. Based on a Likert scale ranging from 0 (not effective) and 5 (highly effective) the experts were asked to judge the remaining practices. This was done with the aim of selecting the best working practices according to experts which in its turn will contribute to solving the problem of the low level of security within organisations. These best working practices could later be used as candidates for the next selection Ease of Design and Realisation, Ease of maintenance and Ease of implementation, also from 0-5. Assessing and ranking all practices over these three dimensions enabled me to comprehensively select the practices which can be monitored and evaluated by the Board (governance level). In consensus with the experts I decided to rank the top practices,

measured from 4 and above on effectiveness. Consensus was achieved due to all experts voting in favour of limiting the number of remaining practices because the aim of the expert research was to derive a core set of high scoring practices. The final list presents a cumulative score of the sum of the score per criterion.

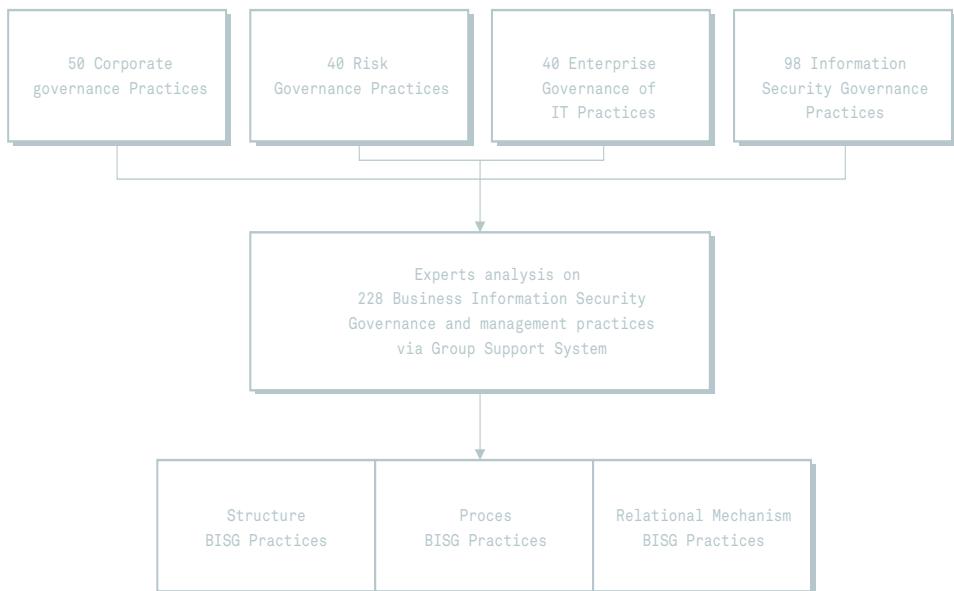


Figure 38: Conceptual model of the literature research, divided into relevant disciplines.

DISCUSSION, LIMITATIONS AND CONCLUSIONS

We can conclude that experts consider the current literature on practices to be rather vague and complex. They supported that view with numerous remarks in the GSS systems during the expert session. This vague or complex formulation of practices might have the result that they are not applied, as Kluge argued in earlier research [4]. Empirical research within 27 organisations also demonstrates this consequence. Some literature suggests more simple and practically-oriented practices – *Report simple (Red-Yellow-Green) and Do simple risk assessments* – with the objective of increasing the adoption of governance practices. The experts also indicate overlap in many practices.

It is interesting to note that there is no sequential order to the list. For instance, the experts rank the effect of "determination of risk appetite" (ranked 7) before "conduct a risk assessment" (ranked 12). Normally, the sequence is the other way around: one cannot determine one's risk appetite if it is unclear where and what the risks are. That is why ranking on effect does not imply a particular sequence. Another example of the limitation of ranking on effect only is the first one of ISG, "Incident response." It is perceived as having much

effect when it is in place but difficult to implement if you do not know who to respond to. The relevant stakeholders first need to be identified (e.g. public, media, regulators) and the appropriate response type needs to be established. This process requires an owner. This practice – “Define ownership” – was ranked 5th by the experts with a 4.5 but was perceived as difficult to implement (score: 2.5).

Our final finding is that the top practices needed to be undoubted as well. An example is “Appoint a responsible and accountable board member for risk management” This can be articulated as determine roles. They both imply the necessity to appoint a responsible and accountable board member for risk management (e.g. technology, information, data risks).

The final list contributes to the academic rigour of security in the absence of proper Business Information Security governance practices and Critical Success Factors. By validating both practical and academic literature on the subject through expert panel research, a more ordered list was assembled in Table 11. This list can function as conceptual framework for BIS. By making a clear distinction between governance and executive management, the practices are applicable in various organisations (independent of a one-tier board or two-tier board). Finally these practices can function as requirements for the business, as well as technical requirements in the artefact. The entire research data including the conceptual framework derived from the literature and GSS expert panel can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

Table 11: Designing and developing the artefact: Top 10 BISG and Critical Success Factors in detail.

#	GOVERNANCE PRACTICE AND/OR CRITICAL SUCCESS FACTOR DESCRIPTION	SCORE	LEVEL	SPRM
1	Determine Roles. Accountability and responsibility for Business Information Security at Board and Executive management level. Including the role of the stakeholders.	11.25	Governance	Structure
2	Corporate internal communication on cyber downside. e.g. cybercrime, fraud, theft, forgery, piracy, bullying. Internal communication channels such as intranet. HRM letters. Workshops can be used to educate employees.	11.25	Management	Relational Mechanism
3	Awareness at level of Boards of Directors. A certain level of awareness about business risks. Business critical information. Level of information (IT) dependency. Kinds of threats from outside and inside.	11.00	Management	Relational Mechanism
4	Board and Senior Management Leadership. Lead by good example. Clean desk policy. Limited personal web exposure (personal blogging, video). Software piracy. Shred confidential papers, etc.	11.00	Governance	Relational Mechanism
5	Lessons learned. Sessions after security incidents. Document and report incidents that occur. Also what kind of response to the stakeholders was made and how such an event can be prevented. Take these in consideration for the formulation of strategy.	11.00	Governance	Process
6	Transparency. The company should also consider the need for a confidential reporting process (whistle-blowing) covering fraud and other risks.	10.75	Governance	Process
7	Determine risk appetite. The level of risk and exposure a company is willing to take when it comes to Information Security Risks. To justify decision-making on investments/insurance.	10.25	Governance	Process
8	Internal control. Regularly review processes and procedures to ensure the effectiveness of its internal systems of control. so that its decision-making capability and the accuracy of its reporting and financial results are maintained at a high level at all times.	10.00	Management	Process
9	Regular reporting on security adequacy and effectiveness. Requiring regular reports from management on the programme's adequacy and effectiveness.	10.00	Management	Process
10	Ensuring the integrity of the corporation. Accounting and financial reporting systems. Including independent audits. Ensure that appropriate systems of control are in place. In particular, systems for risk management, financial and operational control and compliance with the law and relevant standards.	9.75	Management	Process

CONTRIBUTION ARGUMENTS

After compiling the list of BISG practices and Critical Success Factors the goals and requirements were decomposed to articulate a *contribution argument*. This is an argument that an artefact that satisfies the requirements would contribute to a stakeholder goal in the problem context [146].

Example 2:Literature and GSS with experts on BISG						
Method	Intended effect	Side effect (knowledge)	Stakeholder Goal	Artefact requirement	Context assumption	Contribution argument
-Through literature research and GSS the stakeholder group discussed and ranked various governance practices to be relevant for BIS.	-Validating and ranking numerous governance practices from various literature sources -Establish new insights and a structured list.	-Validated literature research. -New insights for the experts. -New insights for the stakeholders. -Insight into critical success factors for improving BISG maturity.	-Have notion and form meaning by governance practices for BIS and its critical success factors. -A prioritised set of BISG practices to measure and maintain BISG.	-A prioritised key set of BISG practices that can function as questionnaires to measure and maintain the BISG maturity.	-Increase awareness by stakeholders (such as regulators), directors and managers. -Increase in knowledge over the BISG maturity state of the organisation. -Take BISG into consideration when reporting on tech risks.	Provide stakeholders with <u>assessment criteria</u> to assess the organisations BISG maturity and provide <u>knowledge and meaning items</u> (i.e. CSF) for Board of Directors in order to direct, monitor and control.

Artefact requirement candidates

The main research question and sub-questions: “*Which practices at the level of governance are relevant for Business Information Security Maturity*” can now be answered. Firstly, security governance practices were investigated. Secondly, the experts ordered these practices and, thirdly, they were ranked.

By doing so, together with the experts I compiled a final list of BISG practices that can function as a frame of reference for Board of Directors. Moreover, this list of criteria may serve as basic parameters of the level of BISG maturity within organisations. Thus, before organisations are able to mature at a governance level, they first need to identify the criteria on which to base their BISG maturity level. For example, if a certain practice is not in place, the indicated level is 0. If it is in place and the existence of the practice can be proved, the initial step towards maturing is made. Ideally, practitioners as well as academia can use these criteria and the proposed method to enhance the BISG maturity of organisations. The top 10 items from Table 12 can function as requirements to be set in the artefact.

Table 12: Designing and developing example 2 of the artefact: Top 20 BISG and Critical Success Factors

RANK	SCORE	GOVERNANCE PRACTICE FOR BUSINESS INFORMATION SECURITY
1,00	11,25	Determine roles
2,00	11,25	Corporate internal communication
3,00	11,00	Awareness
4,00	11,00	Board and Senior Management Leadership
5,00	11,00	Lessons learned
6,00	10,75	Transparency
7,00	10,25	Determine risk appetite
8,00	10,00	Internal Control
9,00	10,00	Regular reporting
10,00	9,75	Ensuring the integrity of the corporation
11,00	9,75	Periodic knowledge evaluation
12,00	9,50	Risk assessments
13,00	9,00	Incident response
14,00	9,00	Identify key information systems and business owners
15,00	8,50	Monitoring and managing potential conflicts of interest
16,00	8,50	Response to risks
17,00	8,50	Risk controlling mechanisms and processes
18,00	8,25	Security as an integral part
19,00	8,00	Identify key risk areas and KPIs
20,00	8,00	Alignment strategy and approval by the board

6.2.2.3 CASE 3: DEFINING BIS MANAGEMENT ARTEFACT REQUIREMENTS

This section was published in the International Journal of IT/Business Alignment and governance (IJITBAG) 1(4), pages 18-39, in December 2010 under the title *A Research Journey into Maturing the Business Information Security of Mid-Market organisations*. The complete publication can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

BACKGROUND AND INTRODUCTION

The problem of the “absence of a core set of interventions” is key. As Workman puts it in his research, organisations are remedied with empirical validated interventions [6]. There are many reasons why we engage empirical exploratory research methods, rather than the more commonly used deductive, hypotheses-testing methods. Primarily because exploratory research is concerned with the generation of ideas [289] and interventions. The problem statement made in Chapter 4 led to the research question “Which core interventions do managers find effective in order to enhance the BIS maturity level?” and this was examined via Group Support System expert panel research. Extra validation was performed in mid-

market companies to increase engagement, as suggested by Workman et al. [6]. This last step was performed to increase the commitment of stakeholders, and to increase the validity of the construct to be established. The final result is a set of interventions which mid-market organisations can apply and these can function as requirements in the artefact.

FROM RESEARCH FINDINGS TO KNOWLEDGE ITEMS

Experts created a top list of interventions from ISO 27002, based on the practicality of each intervention. As a conclusion to the survey research performed in the mid-market segment, I encountered a willingness to implement certain interventions in order to increase security maturity. The following items need to be considered in the design and development of the artefact but are also relevant during the evaluation of the artefact, because they are relevant to improving the maturity of BIS process:

Knowledge items: The barriers "management and organisations" as well as "perception and attitudes" are two categories that scored high in the survey. These were also raised by the experts during the panel as main barriers.

Mid-market organisations state in the survey that involving management would raise their security maturity level. On the other hand, security is perceived as a complex topic and this contradicts the above. How can a security person with the wrong perception advise management on interventions contributing to maturity enhancement?

The survey showed that 22% of the mid-market suggest that 'training and educating personnel on awareness' contributes most to security; this was the opinion of experts according to the expert panel research. The main question remains how to do that in the face of insufficient knowledge and skills.

The experts mentioned during the expert panel research phase that the overwhelming number of applicable laws and frameworks might suffocate the mid-market sector. This seems to be acknowledged by the fact that perception is the biggest barrier and 20% of the organisations do not know that there is indeed applicable law. The mid-market sector has difficulties identifying these, according to the survey outcome. This knowledge item is positioned in the context and scope of the maturing process.

Budget is raised as a barrier by the experts but not listed as an intervention, for example "more money." This is in contradiction to the barrier perception where the intervention is training and educating on awareness. And for the barrier "management and organisation", the intervention management involvement is suggested by the mid-market organisations.

According to the survey "perception and attitudes" is the biggest barrier to the implementation of the third most contributing intervention, risk and impact analysis. An important question for mid-market organisations remains open and that is by who they want to have this risk and impact analysis performed. They have the perception that it is complex

and lack the knowledge and skills to do this.

In conclusion, I state that filling in the survey questionnaire has raised the awareness of mid-market participants. Responses to open questions such as "that's a good idea", "needs to be developed" and "good idea to apply this" proved this.

KNOWLEDGE ITEMS AS PRECONDITIONS FOR IMPROVING MATURITY

The list of interventions presented in Chapter 3 forms a frame of reference for mid-market organisations in order to practically increase business information security maturity. A carefully selected list of interventions presents those interventions that are most effective and easy to implement for a market that, according to the performed survey, struggles with the enforcement of essential interventions. By making use of a combination of ISO best practices and for example the COBIT maturity model organisations have insights into the interventions they have applied as well as those they need to apply in order to achieve a certain maturity level. Translating the most important conclusions of the research into mid-market specific recommendations in order to increase their security maturity, by applying a framework (of interventions, suggested maturity model, organisational preconditions) the research primarily recommends that mid-market organisations:

- Identify applicable (mid-market) laws and legislation.
- Perform risk and impact analysis in order to justify the implementation of necessary interventions in order to achieve the desired security maturity level.
- Apply relevant norms in order to comply with law, legislation or regulations or a framework that is derived from these norms, for example COBIT.
- Involve management in assessing the business impact of not having these essential interventions in place.
- Increase the awareness of security throughout the organisations since human error is the main cause of insecurity. Train and educate with a focus on correct perceptions about security on the technical as well as the business side of the organisation.
- Measure and monitor all potential technical and organisational vulnerabilities (security assessments) as a continuous process in order to be in control and achieve the desired level of security maturity.
- Continuously maintain knowledge and skills that are essential to stay "in control."
- Besides these seven knowledge items, the final results of this empirical exploratory research on assessing, selecting and prioritising a core set of security interventions can function as requirements for the artefact.

CONTRIBUTION ARGUMENTS

After compiling the list of interventions we could now justify the choices for setting requirements. And we articulated the *contribution argument*. This is an argument that an artefact that satisfies the requirements would contribute to a stakeholder goal in the problem context.

Case 3: Defining a BIS maturity assessment						
Method	Intended effect	Side effect (knowledge)	Stakeholder Goal	Artifact requirement	Context assumption	Contribution argument
-Through literature research and GSS the stakeholder group discussed and ranked a core set of management interventions relevant for MBIS. This set was validated and prioritised by the stakeholder target group through a survey.	-Validating and ranking BIS management interventions though experts. -Established new insights and a structured list that was validated by the stakeholder group. -Create commitment with the stakeholder Group	-Validated BoK literature from ISO27K -New insights for the experts. -New insights for the stakeholders. -Insight into relevant knowledge items to consider in the MBIS process.	-Have notion and form meaning through participation in the survey research -collectively establish a core set of BIS management interventions -Via a prioritised set of MBIS interventions to measure and maintain MBIS.	-A prioritised key set of MBIS interventions that can function as questionnaire to measure and maintain MBIS.	-Increase commitment by the stakeholders/ target group -Increase in awareness by stakeholders (such as regulators), directors and managers. Shown by the response of the participants. -Knowledge over the BIS maturity position (current situation) of the organisation and 'to be' situation.	Provide stakeholders with <u>assessment criteria</u> to assess the organisation BIS maturity and provide <u>knowledge and meaningful items</u> (7 preconditions, in order to manage the MBIS process).

ARTEFACT REQUIREMENT CANDIDATES

The design research question: “*Which core interventions do managers find effective in order to enhance the BIS maturity level?*” can now be answered. Firstly, management interventions based on ISO27K were investigated. Secondly, the experts ordered these practices and, thirdly, they were discussed, enriched and ranked. By doing so, I and the experts compiled a core set of MBIS interventions. Secondly these interventions were validated by the target group (stakeholders) to create commitment and increase the validity and reliability of the research. The final list of core interventions is presented in sequence in a flow diagram to indicate the maturity level. This flow diagram is used in the next section of this DS research project when developing the artefact requirements.

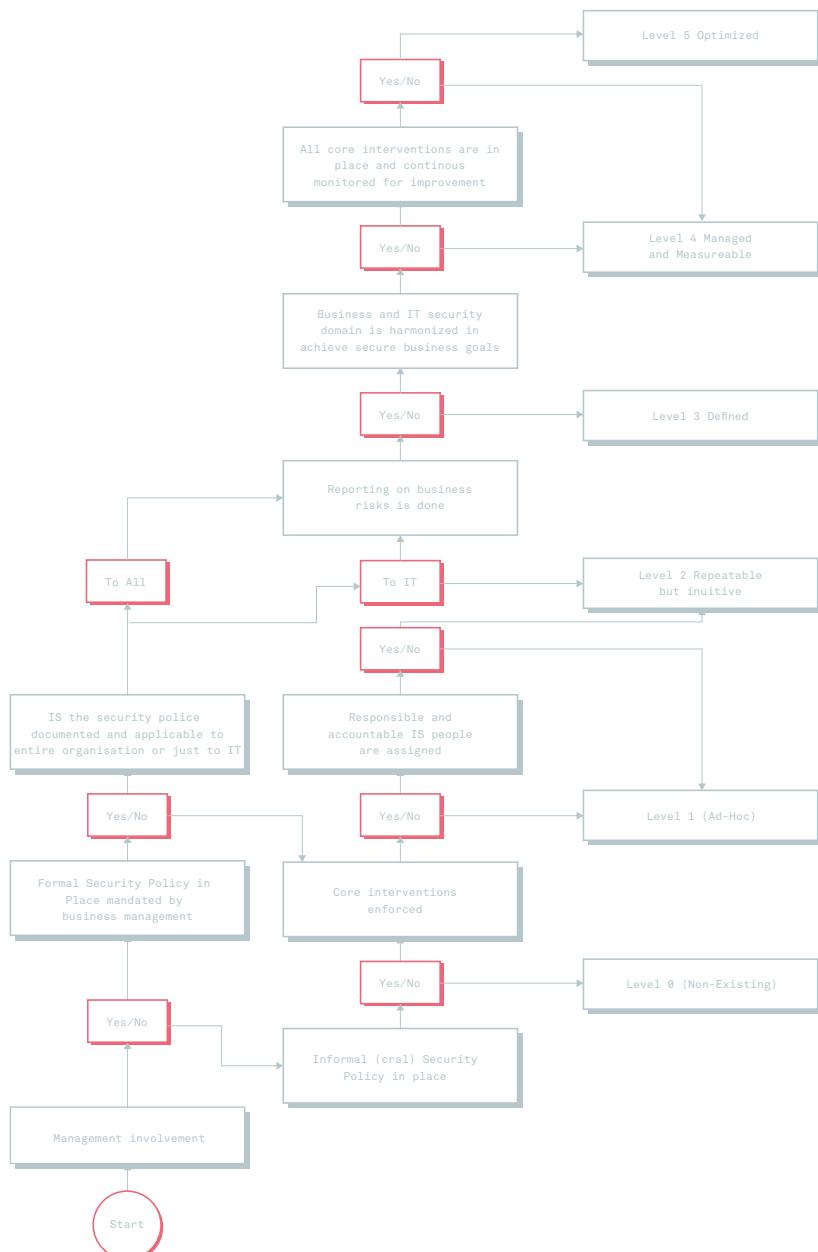


Figure 39: Maturing Business Information Security assessment tree.

6.2.2.4 CASE 4: DEFINING BISG METRICS AS ARTEFACT REQUIREMENTS

BACKGROUND AND INTRODUCTION

To overcome the gap between security professionals and boards in terms of knowledge and language common ground is necessary. Lord Kelvin²⁶ insightfully observed that "*measurement is vital to deep knowledge and understanding in physical science.*" Hence, common ground on essential elements of BIS is needed to gain a certain degree of understanding and consensus. In 2009 a successful contribution to bridging the gap between management and operations was made in the field of Security Metrics by NIST [273]. NIST addressed the necessity of quantifying security for three reasons: 1. *Strategic support*, i.e. in the decision-making process boards need to rely on facts such as historical data, trends and numeric developments. 2. *Quality assurance*, for example using metrics in the software lifecycle development, user access management (i.e. the number of over-privileged users). 3. *Tactical oversight* for monitoring and reporting the security posture of IT systems. NIST also stress the importance of rigorously developing this premature field of security metrics: "*Advancing the state of scientifically sound, security measures and metrics (i.e., a metrology for information system security) would greatly aid the design, implementation, and operation of secure information systems.*" In this research project we explored two major items. One was the metrics per level of the organisation; i.e. operational metrics (operations), tactical (management) and at the strategic level governance and executive management. We explored whether there were adequate metrics, new insights and knowledge that needed consideration in further research. Another item was to explore whether these items are suitable for adopting in the artefact, mainly to measure the MBIS process. As mentioned before, maturity is a process which requires continuous attention and monitoring. So we formulated the main research question as follows: "*Which metrics are effective for governance, management and operational level in order to measure the MBIS process?*"

RESEARCH METHOD TO ANSWER KNOWLEDGE AND DESIGN QUESTIONS

To explore security metrics per organisational level we made use of Delphi research with 38 experts working in the security field. The Delphi method was used to collect qualitative data from individuals and eliminate any form of group influence, in contrast to GSS. In this case the objective was to get experts thinking about which SMART²⁷ metrics they find are suitable for their organisation in order to improve maturity of the BIS process and to generate new ideas. The Delphi method was also used to ask additional knowledge and design questions in. In the first iteration the experts were asked:

1. *Which SMART metrics do you propose for measuring BIS at the level of governance & executive management?*
2. *Which SMART metrics do you propose for measuring BIS at the level of management?*

²⁶ Lord Kelvin (1824) was a British physicist and mathematician of Irish origin. William Thomson is popularly known as 1st Baron Kelvin, the creator of 'absolute zero', which are low-limit temperature units now represented in units of 'Kelvin' in his honour.

²⁷ S.M.A.R.T. is the abbreviation for Specific, Measurable, Attainable, Realistic, Timely

3. Which SMART metrics do you propose for measuring BIS at the level of operations?

RESEARCH RESULTS ON GOVERNANCE METRICS:

1. The result of this first step was a list of 25 SMART metrics. The entire list can be seen in the appendix (in Dutch). When analysing the data set clear process-oriented metrics can be distinguished and these are marked in bold. These can be used to initiate direct, measure and monitor the BIS maturity process.

The relevant items for measuring BIS maturity according to the experts are listed below. The items that relate to the BIS maturity process are marked in bold.

- **Overview of realised versus planned BIS improvements and changes per period**
- **Compliance audit reports per period**
- Percentages of contribution to meeting business goals
- **Frequency of meetings (e.g. steering committees)**
- **Presence of a BIS organisation (steering committee, CISO, CRO)**
- **Business impact analysis (frequently performed) and GAP analysis (on e.g. ISO27K)**
- **Presence of a working risk management process**
- **Presence of policies and guidelines**
- Number of deviation in penalties, incidents and violations (benchmarked)
- **Presence of an audit policy and an appointed auditor**
- **Number of deviations according to the agreed BISG objectives and issues**
- The cost of BIS as a percentage of revenue/profit
- **Level of compliance with internal and external policies**
- Number of business continuity disruptions due to BIS incidents
- Success due to well working security practices
- **Number of audit remarks (for example ISAE3402 or compliance audits) in relation to the SLAs of suppliers and the internal organisation.**

Below are two examples of fresh insights into metrics. Although it's debatable whether they are actually governance metrics, these are perhaps examples of instruments that can operationalise the measurement process. A risk register can be used to monitor the effectiveness of a risk management programme as well as measure and assess the individual risk-related items.

- Risk register and rating against this register
- Reporting security roadmap, incidents, projects and KPIs

Fresh new insights on metrics although it's debatable whether these are governance metrics (and not management or operational metrics):

- Percentage of business-driven innovative programmes where security was involved in an early stage
- Percentage of IT-related projects where security was involved in an early stage
- Number of security incidents.

Encouraging remarks were made by two of the experts: “*I’m seeking good security metrics because currently we only report on our known risks*” and “*If I could have had an answer to all three questions. This is what I’m looking for.*” These last two remarks also show the necessity of this research and the exchange of these insights. It also shows the high level of engagement of security professionals to participate in academic research and confirms the remark by Lord Kelvin at the beginning of this chapter about science being all about its practical application.

RESEARCH RESULTS ON MANAGEMENT METRICS

2. The result of the second step (question) was a list of 24 management metrics for BIS. The most relevant items were filtered out, creating the following clean list of management metrics according to the experts; again the items that address the BIS maturity process are marked in bold.

- **Number of security incidents, effectiveness of security controls, development of the maturity level.**
- **Level of BIS awareness at management level (to be tested).**
- Number of adjustments made to the security baseline during a certain period.
- **Follow ups to previously set KPIs**
- **Working incident management process (#disruptions outside the SLA).**
- **Number of tested BCM plans.**
- **BIS programme progression.**
- The number of new business opportunities that were acquired due to the security proposition of the organisation (Security as a Unique Selling Point).
- **The positive feedback on customer surveys on the security position and trust they have in the organisation. Measure the perception of customers.***
- Number of data breaches per period.
- Customer damage as a result of security incidents
- Number of questions towards the security organisation during a certain period.
- Availability of a full-time security officer.
- Involvement of security at the early stage of projects.
- Achieved CMM level per BIS domain (i.e. physical security, BCM, governance, etc.).
- Time spent on repressive versus preventive measures.
- **Number of audit remarks (for example ISAE3402 or compliance audits) in relation to the SLA's of suppliers and the internal organisation.**

*This fresh idea of getting customers involved in BIS assists the manager in reflecting on the efficiency and effectiveness of the internal security programme. Although this is not directly a process metric it can help to address it. For example, when organisations reach a certain maturity level, they can actively engage their customers in their security programmes.

Examples of ideas that arose during the Delphi research questionnaire but actually are mechanisms used to operationalise measurement:

- Report on the number of risks that occurred during a certain period
- Risk register and rating against this register.
- Examples of metrics that arose during the survey but are indeed more operationally oriented:
- Overview of number of managed end-point devices
- Number of successful entrances (attacks) during a certain time period against the total number of attacks
- Pen-test findings
- Number of (over) authorisations
- Percentage of ex-employee with withdrawn accounts.

The knowledge of the participants was triggered by remarks such as:

These items can be very organisation-specific. He suggested relating the domain of the manager specifically to a certain metric. So he/she does not have to be engaged with all the items.

And again the remark was made: "*I'm seeking good security metrics because currently we only report on our known risks.*"

RESEARCH RESULTS ON OPERATIONAL METRICS

3. The result of the third step is a list of 24 items which is presented below. Again only the most BIS relevant items are adopted, to present a final clean list. The experts raised the following operational metrics:

- Reporting on data from Intrusion Detection Systems (IDS), firewalls (FW), anti-virus (AV) systems and proxies.
- **Number of operational incidents that occur during a certain period**
- Results on Access Control Management (factual figures versus baselines)
- Average detect, response and fix rate on security incidents
- **Level of awareness of security with operational personnel (testing)**
- Percentage of failed pen tests
- **Level of compliance with the security baseline**

- Performance on KPIs
- Number of tested backup procedures
- Number of incidents within or outside the SLA
- **Number of deviations based on the security guidelines (unpatched systems, cleaning of over-authorisations)**
- Number of applications with no security incidents/vulnerabilities
- Percentage of systems that undergo frequent vulnerability analysis
- Percentage of critical perimeter devices/applications and the pen-test results
- **Mean time between failures and mean time till failure as a result of security incidents**
- Average time of security change requests
- Percentage of unpatched systems and active anti-virus software
- Number of business disruptions of the primary business process considered urgent
- KPI on vulnerability management
- Number of resolved versus unresolved security incidents.

The metrics below were raised as operational but are indeed more managerial, perhaps residing within the HRM department:

- Percentage of new employees who followed a BIS awareness programme and the periodically refresh of this programme.
- Percentage of employees with a screening.
- **Number of certified IT personnel**
- Cost of BIS as percentage of revenue/profit
- Employee performance.

The second iteration in the Delphi research was questioning the experts on their opinion on new insights and new knowledge. In other words "*what does this research contribute to them as a security professional?*" Important knowledge gained by the security experts during the research were:

"The complexity of assuring (measuring and monitoring) BIS becomes much clearer."

"There are differences in drivers between government (compliance-driven) organisations and commercial organisations (risk and profit-driven)."

"This research revealed new knowledge and stimulated me to further develop security within my own organisation."

"I have gained new insight into new perspectives on BIS."

Some said they did not get new insights into the topic. This might be the result of using an anonymous form of qualitative research instead of a group-thinking-discussing oriented method, such as GSS.

DISCUSSION, LIMITATIONS AND CONTRIBUTION ARGUMENTS

With the above-mentioned aggregation at an organisational level of metric candidates deeper insight was gained into measurement practices. Not only for me but also the experts

themselves gained new knowledge and were encouraged to think and generate new insights. A limitation in this research is that the experts could not discuss the items. So the result is a messy list of remarks and items that needed proper analysis and structuring. Analysing and reorganising the list was done based on the following viewpoints: Does the answer indeed answer the question? Is there a SMART formulation? (i.e. is it usable for further research?). Some answers were not formulated SMART; indeed most of them were not. Some answers were directives or advice but not metrics. The positive effect of doing qualitative research among these stakeholder groups is the opportunity to capture personal opinions and encouraging remarks, such as the one about the necessity of exploring and summarising metrics.

The final result is a set of BIS metrics which can be applied in measuring and monitoring the process of maturity. In this research project we focus on setting the requirements for the artefact. I did not intend to determine or debate the validity of the metrics in isolation. I also did not intend to create an exhaustive list of metrics. The primary objective was to establish an artefact. Below two metric candidates, per organisational level, are promoted as requirement candidates:

GOVERNANCE

- ◆ Progression in establishing a BIS organisation²⁸ (steering committee, CISO, CRO).
- ◆ Overview of realised versus planned BIS improvements and changes per period.

MANAGEMENT

- ◆ Number of security incidents (via observations²⁹), effectiveness of security controls, development of the maturity level.
- ◆ Number of audit remarks.

OPERATIONS

- ◆ Percentage of failed pen tests
- ◆ Level of compliance with the security baseline.

The entire Delphi research data set is documented in the appendices and can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

28 A security organisation with clear responsibilities, accountabilities, etc. A method used to define roles is a responsibility assignment matrix as RACI matrix (RACI). A RACI describes the participation by various roles (officers, managers) in completing tasks (directing, monitoring and controlling the security function) or providing deliverables within the business process.[4] It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes [328]. In security this functional steering across departments is relevant.

29 In Dutch noted as "bevindingen"

Case 4: The Delphi method for defining BISG metrics as artefact requirements

Method	Intended effect	Side effect (knowledge)	Stakeholder Goal	Artefact requirement	Context assumption	Contribution argument
-Through Delphi research among security managers (sec professionals) new insights were gained on security metrics.	-The insight into metrics assists board of directors and security professionals to create a common ground of knowledge and consensus on importance. -The Raised list of metrics can guide directors in challenging their security staff and set priorities on what they want to measure in order to get in control.	-Create awareness among security professionals on new insights and the use of metrics (the respondents raised their enthusiasms during the participation) -Stimulate security professional to think per organisational level about the relevance of certain data to capture and measure. -Contribute to the rigour with a clear set of metrics raised from security experts with +15 years of experience.	- Insight in measuring criteria and instruments so BIS becomes easier to direct, monitor and control. - Also for external stakeholders to judge if adequate management is done, based on predefined metrics or/and key performance indicators (KPI's). - Gain adequate knowledge which metrics are relevant and how to maintain them.	-Numerous requirements were raised but the focus lies on define the requirements for the artefact that enables the director to measure and mature the BIS process. We defined for Governance: <u>-Progression monitoring on the information security organisation</u> <u>-Progression monitoring on BIS improvements (BIS programme management)</u> On Management; - The number of incidents, effectiveness of the control and number of audit remarks. And on operational level the <u>percentage of failed and passed penetration tests</u> and the level of <u>compliancy towards the security baseline</u> .	-Increase knowledge and commitment by the stakeholders on metrics and the relevant items to measure. -Set priorities for boards in BIS planning and its security investment strategy. -	Provide stakeholders insight into relevant items to measure divided per organisational level. This insight creates a common level of knowledge and consensus on what priorities to set and what to monitor in order to establish a desired state of security maturity. -An evidence-based way of initiating conversations on risk-based priority's setting for security programmes.

6.2.2.5 CASE 5: DEFINING REQUIREMENTS BASED ON PORTER'S FIVE FORCES MODEL

This section has been published in ISACA Journal Volume 1 in 2015 under the title *Porter's Elements for a Business Information Security Strategy*. In this chapter Delphi research is used to define additional strategic requirements for the artefact by making use of the management models of porter. The complete publication can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

BACKGROUND AND INTRODUCTION

Hackers and negative social media hypes have proven able to bring organisations and their perceived value [290] to their knees [291], yet many security professionals (security managers and security officers) lack a clear strategy with clear objectives [56]. The Finn Olav Sveen addresses the importance of socio-technical systems where human organisation and technical factors interact in operationalising the strategy [195], [265] to anticipate and overcome such unpredictable challenges. A Delphi research among forty security managers and CISOs in April 2013 was performed throughout the Netherlands. The security officers were asked a range of questions about the forces they deal with when formulating their security strategy. The main research question was:

What external forces of influence do security managers recognise and how do they cope with them in BIS strategy formulation?

The questions within the survey, which was sent in April 2013, were based on Michael Porter's Five Forces analysis. [277] Porter's Five Forces are a commonly used model to analyse and synthesise how attractive an industry is. Porter distinguishes [277]:

- Competition from rival sellers
- Competition from potential new entrants
- Competition from substitute products producers
- Supplier bargaining power
- Customer bargaining power

This model created by Harvard professor Michael Porter can be used as a frame of reference to examine numerous forces that a security professional can reckon with when establishing his/her 'security strategy.' The experts were asked the following questions and they were able to answer yes or no and with the 3rd question they were able to answer static or dynamic:

1. Do you recognise the following external forces as relevant for BIS?
2. Are you aware of the exact impact of these forces?
3. Do you experience these forces as being static or dynamic?

The following questions were about raising new knowledge items about other relevant forces and the level of influence security managers have on these forces when formulating the strategy:

1. What other external forces do you recognise and experience in your industry?
2. To what extent are you able, as an individual, to influence these forces to your or your organisations' benefit?
3. To what extent is your organisation able to influence these forces to your organisation's benefit?

The last questions were about examining new knowledge that could help security managers do their job better, i.e. formulating a more adequate strategy based on newly gained knowledge.

1. Do you consider it important addressing and incorporating these (for you relevant) external forces of influence in the security strategy and policy in the future?
2. Which industry specific security items (knowledge, experience, skills) do you consider vital for your industry but not for another industry?
3. What would you as an expert provide advice (how to cope with all these forces) so that others can learn and benefit from your expertise?
4. Please explain why your advice is helpful to others?

In the Delphi survey, managers were asked whether the various forces they faced were dynamic or static in nature and whether the managers felt able to bend these forces to their strategic advantage. The results were used to compile a list of suggestions meant to help managers develop a more robust strategy. The complete list of answers is in the appendices.

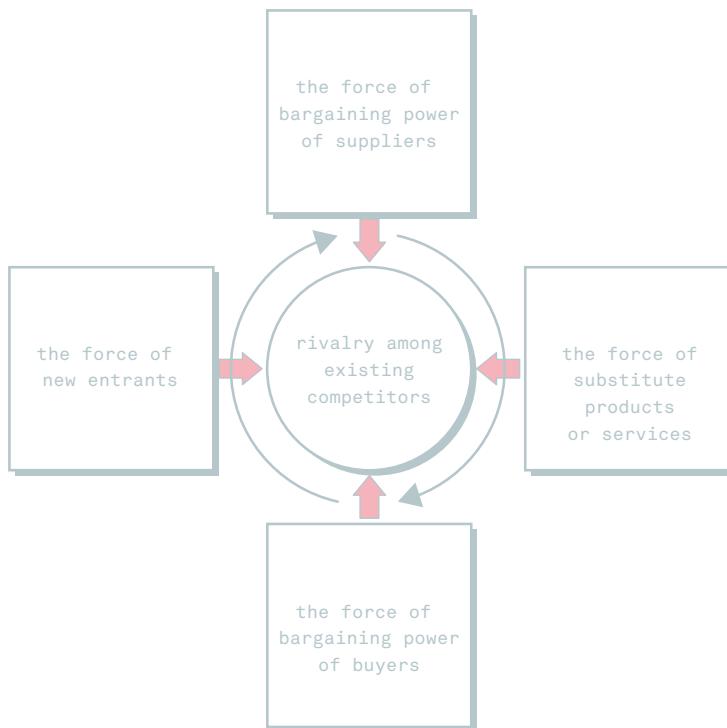


Figure 40: Porter Five Forces model.

 qualtrics.com

The following questions are added because of a parallel research concerning external factors

Michael Porter is a famous strategy professor from Harvard. He developed the "five forces" of influence that shape the organisations' strategy. The exploration and analysis of these external forces seems to be vital in order to develop and maintain a sustainable and profitable model that can be translated into internal policies and working methods. In this research questionnaire we would like to examine if this generic model is also applicable and relevant for the information security strategy of an organisation or even a specific industry.

0% 100%

Survey Powered By [Qualtrics](#) [>>](#)

Figure 41: Screenshot of the Qualtrics survey question about Porter.

DELPHI RESEARCH RESULTS

Two-thirds of the forces security managers said they face are dynamic. In other words, they are unpredictable factors such as intellectual property, property theft, extortion, hacking, social media rumours gone wild and other new-technology phenomena. One-third of the forces they deal with are static, such as compliance legislation, ISO standards and mandatory audits. Nearly 60 percent considered it important to address these external forces in their strategy formulation in the future (they had not done so before the survey). The survey results show security managers focus their strategy on the more predictable, recurrent forces (compliance-related), rather than on the more plentiful and potentially more damaging forces.

BLIND SPOT

In response to the survey the majority indicated that supply chain risk management (e.g. cascade failures due to overlooked forces) should be one of the highest priorities in their organisation. So they understand they have a blind spot preventing them from anticipating risk. But knowing that is not enough. The survey showed that managers are poorly informed about the specific dangers they face and the potential impact of dynamic forces, much less about how they should respond in the event of a full-blown crisis. Nearly 80 percent of the respondents were poorly or only fairly able to influence these forces once they impinged on BIS.

An example of this can be seen through the April 2013 Distributed Denial-of-Service (DDoS) attack that paralysed ING Bank, a global financial institution based in the Netherlands. The incident reduced shareholder value and led to a flurry of criticism via social media, costing ING customers [34]. If the bank had understood and respected the power of such dynamic forces – in this case uncensored social media causing confusion [292] – and been transparent about the attack, the damage could have been limited. Instead, ING denied the seriousness of the attack, evaded questions and remained silent for far too long, [293] allowing the conversation on Twitter to proliferate and leave the lasting impression that the bank had failed to respond. This incident, in addition to many others [294], revealed a lack of preparedness.

CONTAINING VS. AVERTING DAMAGE

Surely, though, it would be better if organisations averted such a crisis in the first place. By the time it was discovered that Impairment Resources had lost control of medical records belonging to the roughly 600 insurance companies it served, the damage was done. The lawsuits quickly piled up and no amount of transparency could have stopped the company's impending demise [295]. So an ounce of prevention is worth a pound of cure.

The results of this survey showed that new knowledge gained via other models can help security practitioners. The survey showed how the Five Forces can be subdivided into dynamic and static forces and how inadequate security strategy is, with its inordinate focus on static forces. The second important result from the survey showed that new knowledge

item such as the five forces and the value chain model can be borrowed from Porter to enrich current strategy formulation within the BIS domain. According to the survey findings, security misses the mark, typically focusing on the individual activities of the organisation rather than considering the role each activity plays in the wider picture. For instance, security specialists see that their business has relationships with third parties, but seldom recognises these parties as potentially influential forces.

Understanding the value chain and the five forces is a prerequisite for business success [296]. Yet, surprisingly, Porter's frameworks have yet to take hold in the BIS field.

These following are ranked out of 13 forces as the top five forces which security managers say they recognise the impact of:

1. Legislation (95 percent)
2. Inspection and supervisory agencies (88 percent)
3. Law enforcement (district attorney and police) (69 percent)
4. Partners in the (digital) chain (e.g., freight forwarders, Internet service providers, payment handlers) (64 percent)
5. Public opinion (60 percent).

The top five forces which security managers say they do not recognise the impact of are:

1. Trade unions (79 percent)
2. Social media (uncensored reporting) (57 percent)
3. Criminals (48 percent)
4. Customers (48 percent)
5. Suppliers (43 percent).

CONCLUSIONS

It is too easy to say that organisations simply need to get a grasp on the dynamic forces in the chain and all their problems will be solved. However, the problem is that very few management tools, steering mechanisms or key performance indicators (KPIs) are available to deal with these forces.

Dynamic forces can have major consequences. A surprising 71 percent of experts surveyed indicated that these forces are critical to their business and security strategy. They require the attention of every manager, board member and shareholder. The survey shows that strategies based on an awareness of value chains and the five forces can help organisational leaders to:

- Increase preparedness for unforeseen influences
- Better identify risk and establish the organisation's risk appetite
- Anticipate crises and remain in control of strategy.

The top five elements for a more holistic BIS strategy, according to the new knowledge insights from the survey, are:

- 1. Stakeholder approach**—When developing a strategy, involve the board of directors, management, business and all external stakeholders in the digital chain. Know the key performance indicators (KPIs), stakeholder expectations, and how to translate these demands, using the right KPIs, into concrete benchmarks for the organisation, management and board.
- 2. Risk-based approach**—Look at the organisation's critical data (crown jewels) in the context of the entire chain. Start by gaining insight into all digital stakeholders and their potential dependencies, weaknesses and risk—both technologically and legally.
- 3. Beware of blind spots**—Many forces are dynamic. Ensure the organisation is not caught unaware. No one person can stay abreast of every development in this field, so let others update stakeholders on what they do not know.
- 4. Do the right things well**—It may seem easier to "learn by doing," but those who prepare a good strategy are less dependent on impromptu solutions.
- 5. Integrated organisational process**—Be aware of the chain of forces that influences the organisation. Make room for addressing these forces in the strategy and policy plans of the entire organisation.

The conclusions of the survey results show that security managers need to zoom in on specific threats and prepare for them; also to zoom out and consider the entire context in which the organisation operates. This is not just a lesson for security managers and officers. It can be argued that the most important decision makers in every organisation need to take ownership of this problem. Information risks are owned by the business data owners, according to ITGI [18] "*It is imperative that organisations deliver on the promise, or they will soon become irrelevant.* [265]" Decision makers should give security people a voice in the formulation of overall business strategy. ICT security policy should be made a core aspect of the whole [56]. Only then can an organisation consider itself ready to face an uncertain and rapidly changing context and future [195].

The entire data set supporting this publication can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

CONTRIBUTION ARGUMENTS

After compiling a set of new knowledge items from the Delphi research we can justify the choices for setting requirements. The gained knowledge items are not directly transferable into artefact functional requirements but they can help influence the stakeholder's perception or have effect on defining the scope and context in which the artefact operates. Although some items are considerable as functional requirements most of the results from this survey are knowledge items to be considered and addressed in scoping the MBIS

process. We use the Wieringa method to formulate the contribution argument. This is an argument that an artefact that satisfies the requirements would contribute to a stakeholder goal in the problem context. A contribution argument, according to Wieringa [146] has the form:

(Artefact requirements) x (Context assumptions) contribute to (Stakeholder goal)

Case 5:Delphi research on knowledge items (5 forces model)						
Method	Intended effect	Side effect (knowledge)	Stakeholder Goal	Artefact requirement	Context assumption	Contribution argument
-Through Delphi research new insights were shared on the use of existing management models to suitable for determining the scope and context of the MBIS process and can function as a set of requirements.	-Establish predefined knowledge items that can function as requirement setting for the artefacts scope and context. -Establish knowledge items on a strategic level to continuously advice board of directors in strategic choices in the BIS domain.	-Create awareness among security professionals on new insights and the use of generic management models. (the respondents raised their enthusiasms during the participation) -Equip security professional with fresh insights i.e. models and language to enable a better dialogue with boards and demystify the security jargon.	-Porters model helps articulate all known relevant strategic forces and opens up the dialogue. -The risk-based holistic approach enables security professionals and their managers to beware of the blind spots.	-Define the strategic forces, address the influence and who's responsible in managing these forces. -The stakeholder approach can function as a questionnaire framed as the <u>"Stakeholder analysis."</u> That can indicate expectations (compliance regulations), risks, KPI's, roles and responsibilities. -Explicate technical and legal dependencies with stakeholders.	-Increase commitment by the stakeholders/target group by making use of existing and well-known models such as Porter. -Anticipate crises and remain in control of strategy -Set priorities for boards in BIS strategy and its investment strategy.	Provide stakeholders with insight into stakeholders and its forces to assess the organisation Security readiness. With the objective to Heighten preparedness for unforeseen influences -Knowledge and meaning items, e.g. 5 elements for a more holistic BIS strategy.

ARTEFACT REQUIREMENT CANDIDATES

Creating insight into strategic forces and the dependency the organisation has on these forces is necessary to:

- Heighten preparedness for unforeseen influences
- Better identify risk and establish the organisation's risk appetite
- Anticipate crises and remain in control of strategy.

STAKEHOLDER ANALYSIS

To identify and analyse the implications of the several strategic forces which certain stakeholders believe should be included in the artefact. In chapter 7 is elaborated how parts of this stakeholder analysis is engineered in the artefact as the function; Information Risk Overview (IRO).

6.3 SUMMARY OF EXPLICATING THE PROBLEM AND DEFINING THE REQUIREMENTS

An artefact can be described by the functions and behaviour [146]. In the previous described examples establishing a checklist of practices, survey or measurement questionnaire to gain insight into practices for maturing BIS is a form of a structure. The establishment of a list, accompanied with surveys, measurement questionnaires and other knowledge items, can assist a director in gaining more or broader knowledge on how to interact with his organisation and its environment and take accountability according to the GDAC theory [211]. And thereby form their personal meaning to their gained knowledge. Lists can be a questionnaire-form with a database connection, that database can store the details of the answers to the questionnaire. The structure of the artefact is designed in a way that the user can fill in the questionnaire, the scales and extra options, so that a direct result is experienced by the user after applying the artefact.

When a board member interacts – based on this new information – with the **environment**, he/she will experience an effect. This can be seen as a direct and intended effect. On the other hand there might be side effects of the artefact making certain items explicit, for example, employees acting in response to certain outcomes. It is my personal experience that after showing factual results of a low performing organisation they immediate want to take action.

All five examples show us that on the one hand new knowledge items to be considered when designing the artefact and on the other easy checklists that can function in the artefact. The end results of all five examples and the outcome in terms of setting requirements is shown in the table below. During this research project the guidelines for design and development of artefacts provided by Johannesson and Perjons [73], were adopted. At the end of this section a summary based on these guidelines is made.

THE ROLE OF STAKEHOLDER IN REQUIREMENT SETTING

In the cases given the role of stakeholders is significant. As participants in the research but also as a target group that could benefit from the artefact. Involving the stakeholder trough the DSR process is necessary in order to assurae the problems are adequately solved. In this section each case is detailed with the specific role of the stakeholder.

Table 13: Summary of five examples and their relationship with the five requirements.

EXAMPLE	RESEARCH STRATEGY/ METHOD	ARTEFACT SOLUTION TO THE PROBLEM	REQUIREMENT	FUNCTIONAL / NON-FUNCTIONAL	IMPORTANT FOR THE STAKEHOLDER
Key BIS management information	GSS	A prioritised key set of BIS management information to use in a dashboard.	Dashboard items	Functional	Because it creates a mutual ground of knowledge, awareness and items to be managed.
Key BIS governance practices and KSF	Literature, GSS and Delphi	A rigorously prioritised set of BIS governance practices to use as a (self) assessment for BISG measurement.	Assessment questionnaire	Functional	Because it creates a mutual ground of knowledge, awareness and items to be governed (evaluated, directed and monitored).
Key BIS management interventions	Literature, GSS and Delphi	A rigorously prioritised set of BIS management interventions to use as a (self) assessment for BIS measurement.	Assessment questionnaire	Functional	Because it creates a mutual ground of knowledge, awareness and items to be managed and frequently measured.
Insight into BIS metrics	Delphi	A set of relevant metrics created by experts to measure and manage BIS.	List of predefined metrics	Non-functional & functional	Because it creates a mutual ground of knowledge, awareness on metrics to consider when managing BIS.
Use of existing management models	Delphi	An alternative view on modelling, capturing and presenting strategic (cyber) forces.	Knowledge items / Defining Scope and context items	Environmental	Because, strategic models such as Porter's can help contemporary CIOs or CISOs overcome the knowledge gap between the CIO or CISO and stakeholders.

1. In the first case the GSS participants are all stakeholders. They are CIOs, CISOs, IT directors or IT managers. So they are considered to be representative in raising information of what upper management or boards want to see as management information
2. in a potential dashboard. They can be considered as a management information supplier or user.
3. In the second case I considered numerous stakeholders during the literature research. Varying from regulator perspectives (COSO, PCI DSS³⁰, SoX, DNB etc.) and accompanying disciplines such finance (Basel2, Solvency, KING³¹ etc.), IT (COBIT, ValIT³², RiskIT). By examining numerous accompanying disciplines such as corporate governance, risk governance and IT governance I established a multi-stakeholder approach, considering numerous views and standpoints. After the literature the latter was judged by GSS. Practices were discussed and prioritised by numerous disciplined experts (architects, managers, consultant, auditor), and this provided another stakeholder perspective (expert perspective).
4. In the third case, a similar multi-method approach was used. I focused in particular on the target group of mid-market organisations. After a rigorously established list gained via GSS expert research, the approach was validated by forty managers of mid-market organisation. By involving the stakeholder directly in addressing interventions that might solve the problem of low security maturity, they thereby also raised functional requirements for the artefact.
5. In case four I asked a large number of CISOs what they find relevant and effective metrics to measure the security. Experienced CISOs can be considered as experts and since they are responsible for the management of security they can also be considered stakeholders. By examining CISOs via the Delphi method the stakeholders are directly involved in solving the problem about the absence of effective security metrics, due to the fact that they collectively raised numerous alternative metrics.
6. In case five I presented the Porter model to the security professionals, in this case professionals within security and not in directing the company. I did this to see if the security professionals were familiar with business world items, such as existing models or methods that his/her manager is familiar with. So in this case CISOs are important stakeholders, to see if they know the model and are familiar with using it. In this case identifying cyber forces that he/she needs to reckon with while formulating a security strategy. So involving CISOs as stakeholders in this research has two beneficial outcomes. First, they gain new knowledge modelling and presenting cyber forces to be considered in strategic plans, and second they develop new knowledge about business world models that is applicable in getting their message across in the board room.

³⁰ The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards (Source : Payment Card Industry Security Standards Council)

³¹ The King Report on Corporate Governance is a code of corporate governance in South Africa issued by the King Committee on Corporate Governance. Three reports were issued in 1994 (King I), 2002 (King II), and 2009 (King III). Compliance with the King Reports is a requirement for companies listed on the Johannesburg Stock Exchange. [256]

³² Val IT is a governance framework that can be used to create business value from IT investments [327]

6.4 DEVELOPING THE SECURIMETER ARTEFACT

The main focus of this Design Science-oriented research project is deriving artefact requirements for solving real-life practical problems that are encountered in business practices, for example, solving the problem of a lack of relevant BIS parameters at the governance level. The problem is the lack of an artefact that captures these parameters and makes them explicit to the stakeholder, such as a BISG checklist in the previous sections. These explicit checklists can assist boards of directors in gaining insight into relevant problem-solving items. So the main orientation of this DS research is *Problem-focused development of artefact requirements* [143].

In this section I continue to elaborate on the previous cases with focus on the development of the artefact see figure below for the position in this research. The artefact can be described by specifying the **function** of the artefact. Thus what the artefact can do for its users in solving a predefined problem. In this example a list of core practices can help boards gain insight, knowledge and measuring criteria. The **structure** of the artefact, thus its internal workings, represents the elements it is built of and how they are inter-related to each other.

Another aspect of the artefact is the **environment**. This is the external surroundings and the conditions in which the artefact will and can operate in order to establish its objectives. The **effects** of the artefact are the way in which the artefact will change the environment. Effects can be intended effects or side effects. In the next section we elaborate the elements that are considered in the design phase and the development phase of the artefact establishment. During the initial research described in Chapter 4 (example 3 in this chapter) the idea arose of constructing a software application that can capture all relevant customer data during the research phase, on current security maturity states and future security maturity states. In the beginning this pilot software was called Maturing Business Information Security Software and was later on named "SecuriMeter." From now on the artefact is described as the technology name "SecuriMeter" or SecuriMeter artefact.

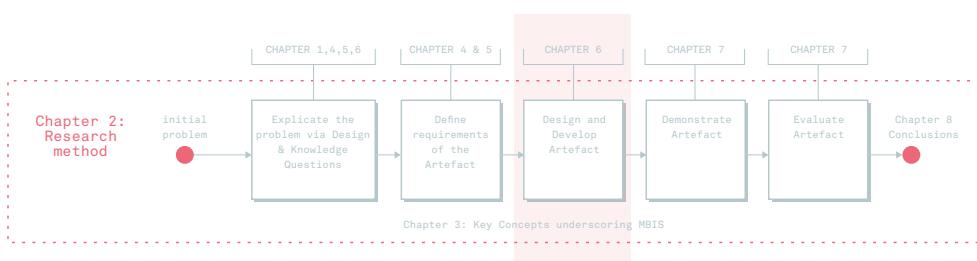


Figure 42: Research phase "developing the artefact" based on Johannesson and Perjons [73].

6.4.1 THE DESIGN AND DEVELOPMENT OF THE SECURIMETER ARTEFACT ONTOLOGICAL LEVEL

In this section a detailed description is made of the basic technical functionalities the SecuriMeter needs to have in order to properly adopt the requirements. Initially to collect data in a database, show the current status, and secondly report that data in a document or other format (dashboard). This should help organisations that want to gain insight into their current and future security maturity state. In Chapter 1 this is framed as the current situation moving towards the desired situation.

The functional design was established through numerous brainstorm sessions in 2010. After the brainstorm sessions between the developer, practitioners and product owner a design was made, based on Unified Modeling Language (UML). UML is intended to provide a standard way to visualise the design of a software system. This functional design is based on numerous iterations between myself and the software developer, starting on 6 August 2010. The entire project of designing, constructing and testing the SecuriMeter application was executed in close collaboration with Utrecht University of Applied Sciences (Hogeschool Utrecht).

The initial kick off of the development phase of the artefact was performed based on two theories; Starreveld et al. Governance, Delegation, Accountability and Control (GDAC) theory [211] and De Leeuw's [213] theory as explained in Chapter 1 and visualised in Figure 43. These theories form the foundation for the brainstorming on business rules setting within the artefact in order to contribute to solving the practical problems already mentioned.

Establish insight into MBIS parameters (metrics, practices, critical success factors, and interventions) that can be set to capture essential fact-based data from the environment on management and operational levels about Planning, Implementation and Control. These governance parameters form criteria to set proper directions (delegation) towards business environments and IT environments (management level) and towards operational plans, implementations and controls. With the objective of collecting the management and operational data (evidence) on these governance practices and achieving control and accountability. This is visualised in Figure 43 where the SecuriMeter artefact is positioned as a governance tool that measures and collects (e.g. administrates) evidence on BIS.

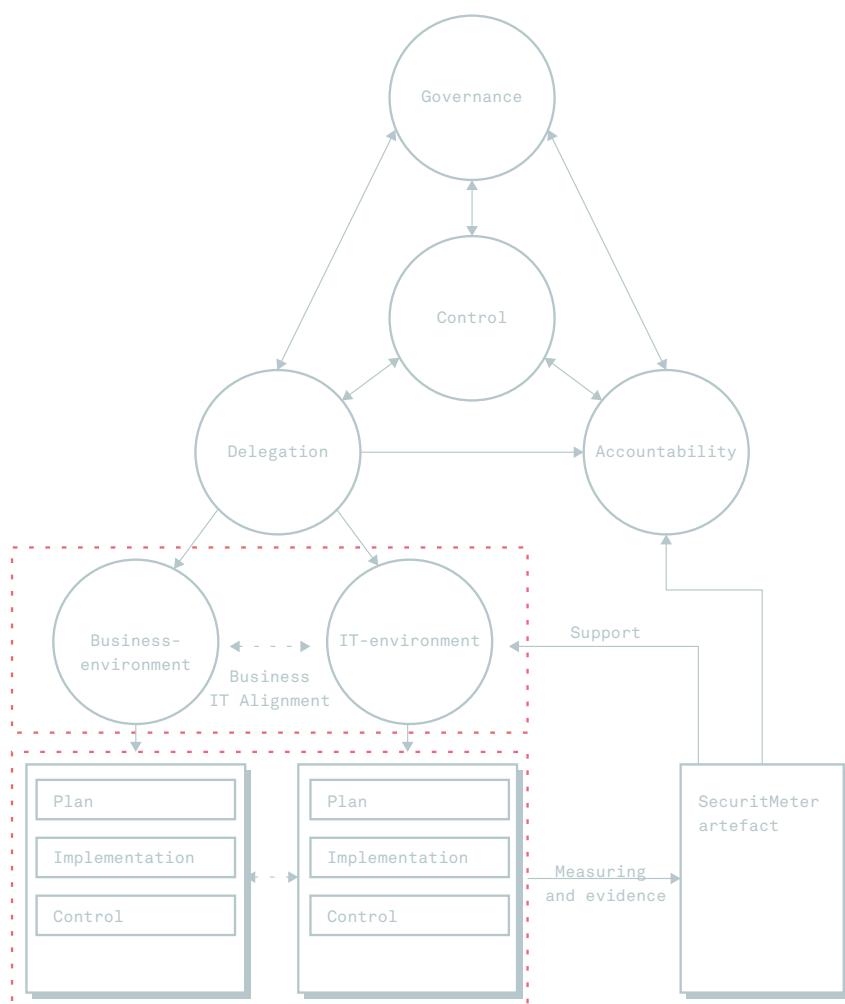


Figure 43: Positioning of the artefact's based on Starreveld et al. [211] and De Leeuw [213].

6.4.2 THE DEVELOPMENT OF THE SECURIMETER ARTEFACT ON INFORMATIONAL AND DATA LEVEL

This section describes the functional requirements for the application. The functionalities are described as use cases and also describe the requirements and results of these actions. The detailed use cases and results are in the appendix. The basic concept of the application is to aid consultants in performing their security audits, assessments, reviews (i.e. business research). The application will make it possible to enter data collected at customers into the application which allows the consultant to create a report based on the data and grant a score to the test (and company). The questions and the assessments that are taken will be maintainable within the system. The assessments can be branch specific. The assessments will contain help texts for the questions (to aid the person entering) and can contain advice when the requirement is not met. The application will also make it possible to maintain clients and their information. The system allows the entry of customers and the maintenance of their information. It is also possible to view the taken assessments. The clients will be placed within (maintainable) branches. The selected branch also limits the tests which can be taken for that customer. Also support for (limited) reporting will be built in. By analysing the data in the system reports can be generated about tests (how many were passed) or about branches (which tests are taken and which results were reached). The application will not implement automation of test tools (i.e. vulnerability scanners) since this can be quite complex and we in that case need to rely on certain software which can give issues regarding licensing. The system however can give advice regarding tooling and the interpretation of the data, but will rely on human judgement to determine whether a certain requirement/question is fulfilled.

The users of the application can be placed in groups which will be granted user rights. To enforce security and confidence confidential information will be stored encrypted. For this document we assume that the user executing the use case has the correct rights to be allowed to access this functionality. If a functionality will behave different according to the rights this will be noted in the use case.

Figure 44 shows how the application will function in terms of the primary processes of the consultant (named B-Able):

MODULAR APPROACH

The artefact application needs to be divided into separate modules. The application use can be limited with user rights. The following modules are defined in the artefact application (the name artefact and application is being used in mixed terms and implies the same):

- Administration module
 - Maintain branches and industry types
 - Maintain users and user groups (+rights)
 - Maintain application base data

- Relation management
 - ♦ Maintain customer data
 - ♦ Perform quick scan
- Assessment management
 - ♦ Maintain questions and question lists
 - ♦ Maintain assessments
 - ♦ Maintaining assessment versions and types and assign them to branches
- Assessment module
 - ♦ Take assessments
 - ♦ Generate reports about assessments
 - ♦ Rating of the assessment by the user and uploading final report
- Statistics
 - ♦ View statistics per assessment
 - ♦ View statistics per branch.

The full UML based functional design is in the appendix

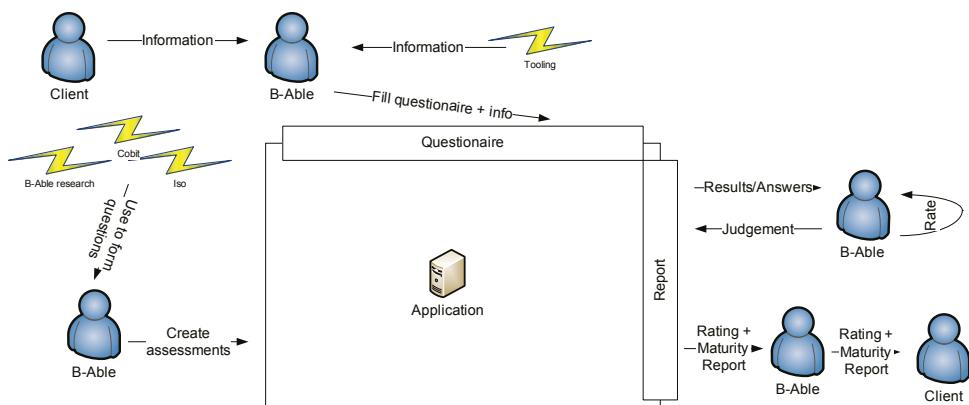


Figure 44: Design and development: the functional design of the MBIS artefact.

6.4.3 FROM INITIAL FUNCTIONAL DESIGN TO PROTOTYPING

This section describes the technical and architectural part of the application after the first iteration of the functional design (25 August 2010).

ARCHITECTURE

The final application (within the first phase) is built as a two-tier application. This means that the application has a database layer and an application layer. The application layer is the client application running on the client's computer. The database layer is the SQL server instance which is hosted centrally. The client application will directly connect to the SQL server database (via an encrypted data connection). The code within the client will be written in a two layer structure. The graphical representation and the business logic within the application are split to make future splitting of the layers into physical layer possible (like for example the creation of a central web service, the clients communicate with for business logic).

Encryption

Sensitive data between the client application and the database was encrypted. Data was sent encrypted to the database which stores this encrypted data. The database therefore only contains encrypted data. If data is retrieved from the database it is decrypted on the client. This solution however has one downside, being that we cannot use the search/indexing possibilities of SQL server. Searching for a certain company name by, for example, a part of its name will not be done on the SQL server but must be done on the client (after decryption of the data). Also encryption/decryption can slightly reduce the performance. However we consider both downsides acceptable due to the nature of the data in the system being confidential and the main target is to ensure the confidentiality and integrity of this data.

TECHNIQUES

The application will be written in the Microsoft .NET 4.0 framework. The Graphical User Interface will be implemented in Windows Presentation Foundation (WPF), supported by Windows Vista, Windows 7 and partially supported by Windows XP. Data storage will be done in Microsoft SQL Server (2005 or 2008). Communication between SQL Server and the .NET application is done via a wrapper around the default communication protocol of .NET with SQL server which will contain logic for encrypting and decrypting information send to and received from the database. In the application design phase we also considered the items we might want to add in the future. This section describes the elements we have identified in 2010 as possible future improvements.

LICENSING

In future we want to have the ability to valorise this research project by selling the application to businesses. This is identified as phase 3 of the application implementation. To enable licensing of the application a wrapper will be created to check whether the licence is valid. Another important consideration in the resell version is the necessity of shielding certain

functionalities, due to confidentiality. During that phase of development we also need to reconsider rollups of the code. When a new version or assessment is released, we need to roll these to the customer versions of the application. In the third phase of the application we need to make a plan how to do this without violating the user data.

SOFTWARE AS A SERVICE

One possible way of reselling the application is to enable Software as a Service (SaaS). With this technique the users will not receive a physical copy of the application, but can use the application from a server. Preparation for this version is done by splitting the application into separate layers from the start. By splitting the database, logic and Graphical User Interface (GUI) we were able to create a new GUI (possibly web-based) for the SaaS implementation.

AUTO INTERPRETATION OF ASSESSMENT SCORES (AND GIVE A RATING)

The first versions of the application will not support auto interpretation of the assessments. This is due to the complicating factors when rating a list. Whether a test is passed relies on certain factors (like a minimum score, or the compliancy of at least x items, the compliancy to require at least a certain (set of) item(s) or a complex combination of this. The basic prototyping functionality of the application is to store the important customer data and keep track of assessments. In collaboration with the developer I decided to leave the interpretation of the results also to a human, since a human is better in determining which requirements can cause a test to fail. The person will rate the list (with the answer report list we generated from the system) and will enter his rating and findings into the system. The system will store the rating and findings with the assessment. In future versions it might be possible to let the system interpret the answers and come with a score.

This first iteration of the functional design in August 2010 led to building and delivering a prototype version.

6.4.4 THE STRUCTURE AND THE TECHNICAL SPECIFICATIONS OF THE ARTEFACT

In this section we elaborate the technical specifications and functionalities of the SecuriMeter artefact. Since the SecuriMeter is a software application we will switch terminology between, tool, application, where we mean the SecuriMeter artefact. The description is based on Dynamic Systems Development method (DSDM), a form of Agile software development. This DSDM method is based on multiple iterations between myself and the software developers. This description is established on numerous writing and building iterations, data and designs dated May 2013 (version 3.7.4). This specification describes the various used techniques within the application source, the libraries used and the layering of the application.

TECHNICAL DEPENDENCIES

The system is constructed based on Microsoft .NET technologies. For the Windows front-end the user should have the correct version of the .NET framework installed. For data storage it relies on a SQL Server 2008R2. To store the data the application landscape should have at least one SQL server instance installed (on a user level or on network level). The Windows client should support Microsoft .NET Framework 4.5³³, SQL Server Edition 2008R2 for Offline mode. For the web server the Microsoft .NET Framework 4.5 and IIS 7 or higher (requires Windows Server Internet Information Services/Webserver Role) is required. The web client should be Internet Explorer 8 or higher. The Central DB server³⁴ should be SQL Server Edition 2008R2 (Express edition is supported). The system is compiled processor/architecture independent meaning that x86 (32 bit) and x64 (64 bit systems) is supported. This visual presents the conceptual infrastructure model of the SecuriMeter artefact.

The application supports 2 interfaces, a web interface and a windows interface. The web interface is exposed through a Microsoft Unified Access Gateway (UAG) security technology layer which allows clients to login with their browser and access the application. There is also support for a Windows front-end for the consultants that are connected to the local network or connected via a Virtual Private Network (VPN) technology. The Windows interface supports assessment taking and system management where the web interface only supports assessment taking and reporting for one client-relation³⁵.

When logging in on the UAG the users will get a Lightweight Directory Access Protocol (LDAP) security token. LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network which will be forwarded to the website. The website will determine the login by looking at the LDAP token. The Windows front-end supports LDAP login, but is also supporting login by username and password.

Users that are not directly connected to the network can use the offline mode of the application. This allows a user to work offline and sync his changes when needed³⁶.

6.4.5 SYSTEM LAYERS IN THE ARTEFACT

The SecuriMeter application is divided into numerous layers. This allows us to respect the single responsibility principle and makes it possible to replace layers (or items) in a later phase of the project. The diagram in Figure 46 shows the main layer groups and the specific layers that are part of the groups.

³³ 32 and 64 bits compatible, the code is compiled architecture independent

³⁴ The central DB server is the server used when numerous consultants want to use the tool with centralized data. It is not required since the system also supports working on a SQL instance on a client machine.

³⁵ A user can have rights in multiple relations, but for the web access only one relation is allowed per user.

³⁶ For more information about the offline mode please refer to the offline mode section.

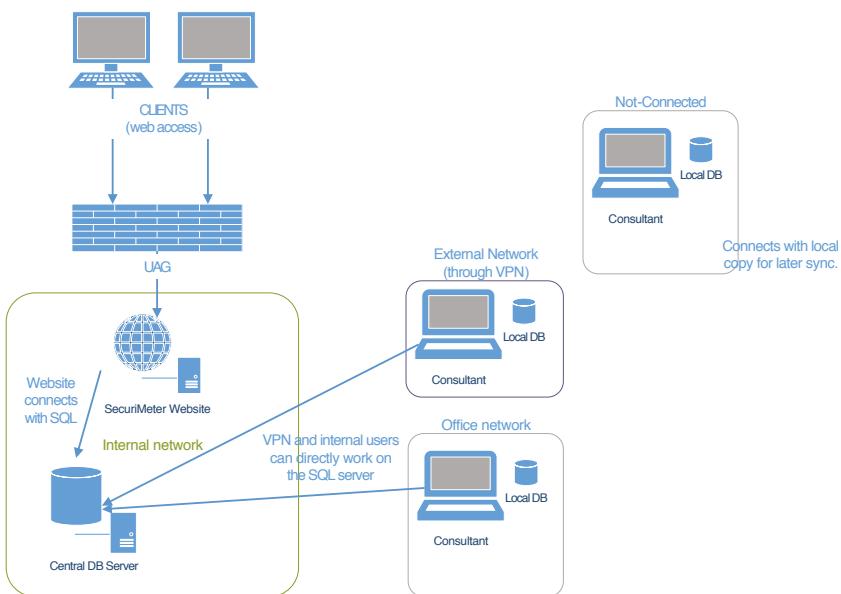


Figure 45: Designing and developing the artefact: The technical design of the artefact infrastructure.

6.4.5.1 GENERAL USAGE

The general usage layer is a layer of components used throughout the whole system. The elements here are available in all layers and can be used to communicate data through the layers.

The *SecuriMeter.Library.BE* project contains the business entities. These entities are objects to store data. The objects in this layer serve as data containers and will communicate data between the logic layer and the front-end layer and are also used by the front-end to display or communicate with other parts of the layer.

The *SecuriMeter.Library.Util* project contains helper functions which need to be exposed to several layers. Helper functions are functions such as validation of certain objects, core classes, formatting classes, etc.

The system is also using some *external libraries* to perform certain actions. The following external libraries are part of the application:

VHCD.Library.Database³⁷

This library is responsible for the communication with the database. This simplifies the usage

³⁷ This VHCD Library is a proprietary library

of the default .NET connection capabilities.

Microsoft.Office.Interop.Excel and Microsoft.Office.Interop.Word

This is used to perform Word/Excel export of reports.

6.4.5.2 DATA LAYER

The data layer is the layer which stores the data. In the SecuriMeter application this is a SQL Server database. Communication with the database is done through the Business Logic Layer³⁸. The database tables are accessed through stored procedures.

6.4.5.3 LOGIC LAYER

The business logic layer contains all the logic for the application. It contains logic about how to access certain data in the data layer, but also contains logic to determine assessment scores or perform an assessment export.

The SecuriMeter.Library.BLL layer contains the communication logic for the data-access layer and contains logic to store and read items from that layer. The BLL will use the BE objects to store/load data and will perform basic validation on these objects. The BLL is also able to distinguish the offline and online mode and communicate with the corresponding database. The BLL library uses the VHCD database library to communicate with the SQL server database.

The SecuriMeter library contains logic which is not directly related to the database. This layer contains objects with logic that is used by the various front-end components. Elements in the library are the import and export of Word/Excel documents, authorisation handlers, etc.

6.4.5.4 GRAPHICAL LAYER - FRONT-END

The front-end layer contains all items that display or process data for/to a user. This can be Graphical User Interface (GUI) but also interfacing applications, updates, tests suites. Each layer that can produce an output or read an input is seen as part of the front-end layer. Items in the front-end layer mainly only serve as a display layer and therefore should contain little to no logic except from graphical flow logic.

The web front-end is the ASP.NET website that can be used by clients. This site uses the generic library and business layer for implementation of logic. The Windows front-end and Windows controls projects contain the graphical logic of the Windows front-end of the SecuriMeter. The control project contains controls such as buttons, grids, etc. which can be re-used over multiple Windows front-ends to ensure consistency.

38 Exception to this is the DB Updater; this specific part of the application will perform

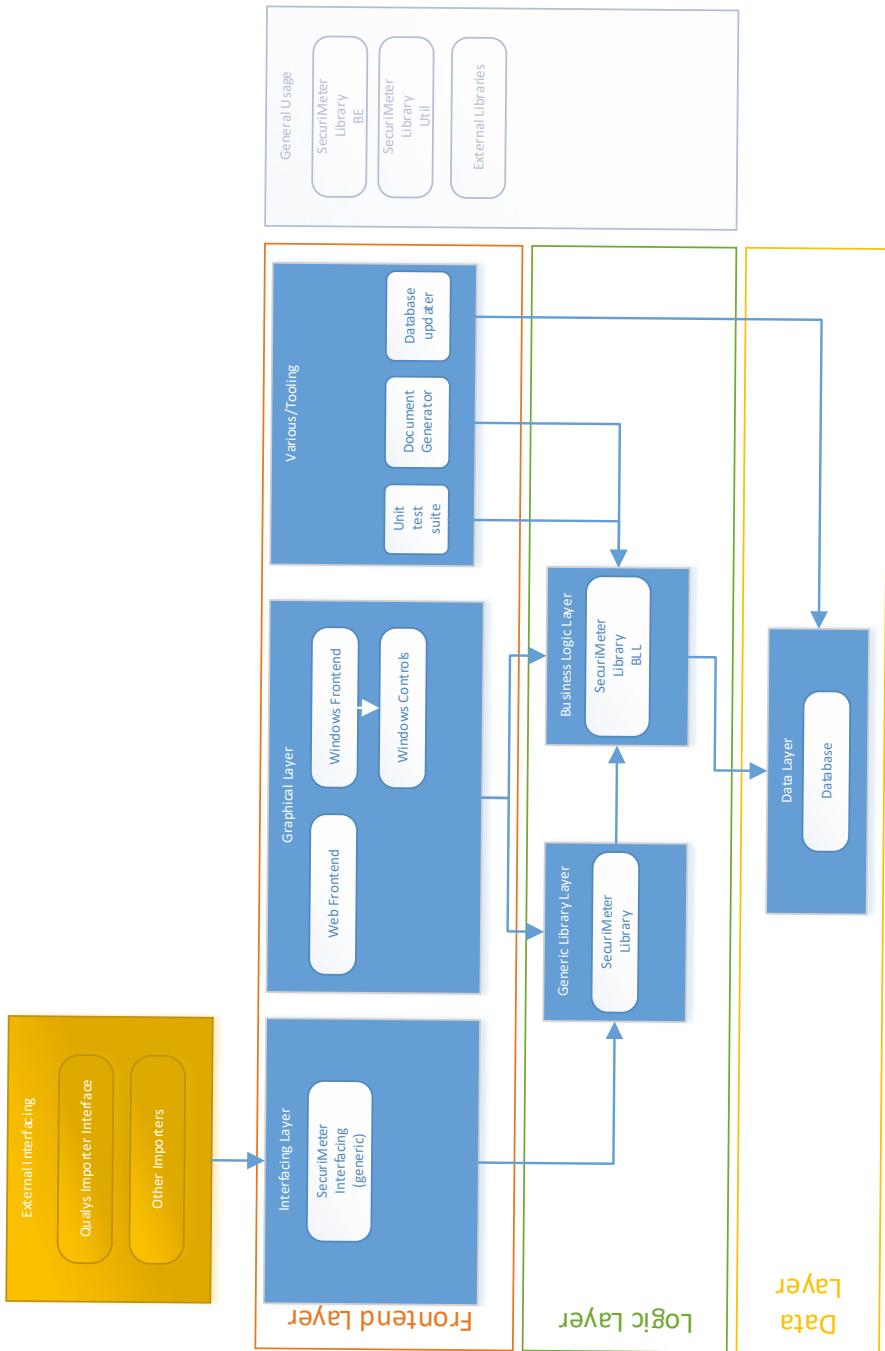


Figure 4.6: Designing and developing the artefact: different layers in the artefact.

6.4.5.5 INTERFACING LAYER (AND EXTERNAL INTERFACING)

The interfacing layer offers a way for external interfaces to use some (but not all) logic from the SecuriMeter application. The interfacing layer allows developers to plugin new functionality in the system³⁹. The interfacing logic in the application will scan for usable plugins and will be able to call these interfaces. Within the interface logic are a set of interface descriptions which must be implemented in the plugins. By knowing the interface definition the system can easily call plugins and let them do the job.

The plugin interface will provide de necessary data to the interface implementation and the implementation will return an updated set of data (together with processing information) to the SecuriMeter application. The plugins should never use business logic or data communication with the other layers of the system and should never perform data manipulation at the data layer level.

6.4.5.6 VARIOUS FORMS OF TOOLING

The project contains a light test suite which contains functions to perform automated tests on the application layers (library/bll/data). These tests will be run before releasing a project to ensure the working of the tool⁴⁰. The document generator functions as front-end for the generation of Word template reports. This uses the logic layer to perform lookups and write the export document. The database updater directly works on the database. This updater can be used to update production/test databases to the new version. It will implement new tables, update or create stored procedures and if required will perform setup of initial data or update existing data to match the software requirements.

The update contains updates for each version (since 3.5.0) and will run a cumulative update.

SPECIFIC PARTS

This part will describe the functional and technical side of some of the specific parts in the system. Each of these parts forms a core part of the SecuriMeter application landscape.

6.4.5.7 DOCUMENT GENERATOR

Because of the limitations of the reporting engine, which is using Word Interop, it is not possible to directly generate reports in the web front-end. Microsoft advises against the usage of Word Interop on web servers because of potential security risks and performance loss. Also the licence model of Microsoft Office does not allow the use of web servers. To work around this issue we developed a document generator. The website will queue a report in a reporting queue which is monitored by one or more Document Generators. The generator will run on a separated machine and will pick up each report for processing. After processing

39 Currently only applicable for tooling answer import (Qualys Vulnerability Scanner)

40 Unfortunately not all functionality is tested by this test suite yet. The test suite will be expanded with extra functionality tests during further development of the application.

the tool places the file in the database and signals the website (and the client) about the file being ready for download.

6.4.5.8 OFFLINE MODE

To support working with the tool when no internet connection is available⁴¹ we implemented an offline mode. The offline mode will synchronise the data from the production database. For the offline mode the system uses a SQL Server Express edition instance on the client machine. This will attach the offline database file and use that in the offline mode. The offline DB is also attached when entering the synchronise mode (both ways). In that mode the system will read the data to copy/update in the memory and attach the destination database to copy the data.

The offline prepare will take an empty database and fill it with data. The prepared database is stored as offline database in the application folder.

6.4.5.9 EXTERNAL INTERFACING

To be able to communicate with other system we introduced the concept of external interfacing. This includes (or will include) possibilities for other systems to communicate with the SecuriMeter tool or possibilities for SecuriMeter to communicate with other systems or interpret the data from those systems. Interfacing can be performed on 2 levels. First people can communicate with the business logic layer of the application. At the moment this will mean communicating/linking with our DLL, but in the future we might want to expose some of the functionalities through (web)services/APIs⁴². The other option of interfacing is through the interface capabilities within the SecuriMeter interface, the system can offer various ways to load DLL's that facilitate interfacing. Currently the method is used to facilitate interfacing in the assessment taking screens⁴³.

6.4.5.10 LDAP INTEGRATION

The system supports the login through LDAP. When configuring a user the administrator can supply a LDAP name of the user. When LDAP is enabled the system will look for the LDAP token of the user (works in the web and Windows application) and look in the system if this token is assigned to a valid user. This way the system can login these users without requiring them a different login for SecuriMeter. For web the LDAP login is mandatory since the website does not support login with a username and password. The LDAP token is provided by the UAG when the user successfully logged in on the UAG with his credentials.

⁴¹ In certain cases the consultants are not able to connect to the network while at client's location due to limitation or security regulation.

⁴² Here data will be pulled/pushed by the consuming applications

⁴³ With this method the SecuriMeter will be pushing/pulling data

6.4.5.11 TWO VARIOUS BUILDS (ADMIN/NON-ADMIN)

For the system there are two different builds. There is an admin build which includes all functionalities and a consultant build. The consultant build is equal to the admin build but has the user administration part removed from the GUI. This is done to prevent accidental changes in the consultant mode.

6.4.5.12 SQL PASSTHROUGH

Microsoft.NET, and thus SecuriMeter, allows the connection to the database to use the credentials of the Windows user. This can be used to obfuscate the connection credentials to the database and to create an extra security layer. For the consultant versions the SQL pass through is enabled in the configuration file. To enable users to connect to the database through their Windows credentials the system supports functionality to link the user account in the SQL database server and assign the correct rights to that user.

6.4.5.13 FUTURE CONSIDERATIONS FOR SECURIMETER DEVELOPMENT

In future we can consider the following technical changes to the application.

LOOSEN COUPLING BETWEEN THE LAYERS

At this moment the business logic layer is tightly coupled to the presentation layers of the application. This makes it difficult to "quickly" replace the logic layer within the presentation layers. This is not a direct problem; however the current best practices describe a model where we programme against an interface instead of an implementation. In the future we might consider applying this practice to the logic layer for consistency and maintainability.

USE AN INDUSTRY-STANDARD DATA-ACCESS METHOD

In this current version in house developed database layer is used. This relies on the default data readers from .NET and uses stored procedures to communicate with the database. While this control is just an additional layer on the default working of .NET (and only serves as helpful portal) we might consider using a different database connection methodology (like Entity Framework) to lessen the development of database calls and be able to rely on new cutting-edge technology. However, making this change might require a fierce rewrite of the business layer's communication with the database.

ENRICH AUTOMATED TESTING

Some of the functionalities in the application are tested through automated test scripts; however not all were tested in these scripts. During the current development cycles we try to extend the automated tests with test cases for the newly developed functionalities (only the logic is tested, GUI's cannot be tested). We might consider adding test cases for some of the existing functionalities to ensure the working of the current system in future releases.

6.4.6 ADHERING TO THE GUIDELINES FOR ARTEFACT DESIGN AND DEVELOPMENT

During this research project the guidelines for design and development of artefacts provided by Johannesson and Perjons [73] were adopted. These are:

- *Clearly describe each component of the artefact.* This is done with the functional and technical design layout in the previous section and in the UML use case design in the appendix.
- *Justify each component of the artefact.* Explaining the purpose of each component of the artefact in particular which requirements it addresses is expressed in the UML use cases.
- *Describe the use of the artefact.* This is demonstrated in the UML use case diagrams in the appendix.
- *Clarify the originality.* The originality of the artefact is in the combination of the input, in this case for example governance practices or management practices that contribute to solving the problem of MBIS, and the implementation into the artefact in the form of questionnaires which can be validated by proof, i.e. parsing operational security tool data.
- *Specify the sources of the design of the artefact.* In the pre-definition of the requirements and problem articulation the role of the stakeholder and its input is considered. In the section on the role of the stakeholder is elaborated how he/she is involved into setting the requirements. In the example of the Porter model to gain new knowledge on intended forces worked inspirational to the stakeholder and/or inspired the design of new components.
- *Describe how the artefact has been designed and developed.* This explains what has been done to design and develop the artefact, in particular how the stakeholders have been involved and how existing solutions and research literature have been reviewed.

6.4.7 ARTEFACT DEVELOPMENT AND MAINTENANCE

In order to log development issues during the development phase an issue log was established. This issue log is also used as directory of future requirements that were raised. It enabled me to track and trace the development of the artefact based on software release notes. An extract of the initial issue log is shown in the table below. This issue log was initiated after the first official release on 8th April 2011. The initial pilot version of the artefact was released in March 2011.

Issuelog SecuriMeter tooling

Nr	Date	Prio	Raised by	Status	Client	Release	Description (Dutch)	Remark
1	24-3-2011	Middel	SP	Done	Yes	v20110325	Mobile phone bij contact feilgenvens	
2	24-3-2011	Middel	SP	Done	Yes	v20110325	Bij save niet de assessment daalwe de relatie duuren,-verwend	
3	24-3-2011	Middel	SP	Closed			Scherf kan niet kleiner dan 2/3 van mijn scherm!(204*768 old?)	Gesloten, vanwege schermopmaak niet wenselijk kleinere te maken
4	24-3-2011	Middel	SP	Open			Niveau's is expand? Misschien niet drieënkele old?	Niet meer relevant (verwijderen)
5	24-3-2011	Middel	SP	Open			met niveau's is expand bedoeld ik dat je bijvoorbeeld 1 reetwerk groep kan expanderen, en de rest niet... (test praktisch als je iets van 200 vragen erin hebt staan nameijk...)	
6	24-3-2011	Middel	SP	Done	Yes	v20110401	Als je expand... graag scherm bij dezelfde in de lijst hangen voor grote vraaglijsten zeer praktisch	Niet meer relevant (verwijderen)
7	24-3-2011	Middel	SP	Done	Yes	v20110401	Is het mogelijk om een onderscheid te maken tussen vragen door middel van bijvoorbeeld een coort knop?	
8	18-3-2011	Middel	SP	Done	Yes	v20110325	Wijzigen volgende vragen, groepen en antwoorden	
9	18-3-2011	Middel	SP	Done	Yes	v20110325	Nieuw scherm, soort van control panel per relatie waar meter op staat van het huidige security level, gewenste security loven en een grafiek old voor het verloop van de afgelopen tijd. Meter zoals in plastic ondertek. [40.5 hoge, 10 laag] [Hieruit kan je ook een selectiescherm van de relaties dubbelklik voor openen, dan schermvullend de naam van de relatie, ja niet! NG open, als je bij de Rabobank zit, voorbeeld) en dan een knop, ja, openen, nee, kies andere relatie, dan naar het control paneel van de Rabobank.	Grafiek is new version dashboard inclusief maturity level "Hockey stick" is aangemaakt, te bestuderen via de knop op het hoofdscherm. Relatie beheer wordt door het gebruik van het dashboard niet meer aangesloten bij blanen, dit is besproken. De maturity levels worden ook alleen in het dashboard getoond.
10	18-3-2011	Middel	SP	Done	Yes	v20110325	Wilt een relatie graag wissen per contact met 1 klik, [vo dubbeltik]	Wat moet je nou typelijk het contact opstellen als je een ander heeft te maken met de positionering van de controls, je kunt het niet te maken.
14	18-3-2011	Middel	SP	Done	Yes	v20110408	De knoppen "Delete contact & Save contact" vullen over "Add contact" als het scherm	Hef je op next druk in de quickscan zonder een antwoord in te vullen komt er een SQL error. [pv melding dat er iets ingevuld dient te worden]
15	18-3-2011	Middel	SP	Done	Yes	v20110325	In de quickscan een on-a-klaaste vraag: "na" moet "to" zijn	Geen SQL error, maar indierdaad wel een foutmelding. ik had een foutje in de code, hij had een melding moeten geven dat
19	18-3-2011	Middel	SP	Done	Yes	v20110325	In de quickscan een on-a-klaaste vraag: "na" moet "to" zijn	
20	18-3-2011	Middel	SP	Done	Yes	v20110325	In de quickscan, laatste vraag: coninc U dus	
21	18-3-2011	Middel	SP	Done	Yes	v20110325	Een veld met suggestie per vraag en het opslaan in de database voor veranderen/verbeeteringen)	Bij iedere vraag is een knop gekomen om een suggestie in te leggen via een nieuw scherm, als je daar kiest voor submit zie 25
22	18-3-2011	Middel	SP	Done	Yes	v20110325	Optie om eens per maand old die suggesties uit te lezen zodat er verbeteringen of veranderingen kunnen worden doorgeworerd.	
23	18-3-2011	Middel	SP	Done	Yes	v20110325		

Table 14: Extract from the SecuriMeter issue log.

6.5 CONCLUSION TO THE DESIGN AND DEVELOPMENT OF THE ARTEFACT

Ultimately a set of artefact requirements were established through a design science cycle. In Cases 2 and 3 this was done via numerous iterations and numerous methods. Table 15 highlights the final requirements to be adopted in the technical design of the SecuriMeter artefact. According to Wieringa, non-functional requirements are operationalised by indicators [143]. In the next chapter we elaborate on these indicators and norms to indicate the direction of improvement within BIS.

A demonstration of the artefacts working can be viewed via the video on the appendices and can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

Table 15: Summary of the 5 requirements in the artefact.

CASE	REQUIREMENT	FORM
1.Key BIS management information	Dashboard on policy status, risks and evidence	Dashboard
2.Key BIS governance practices and KSF	BISG Assessment questionnaire	Functional
3.Key BIS management interventions	BIS maturity assessment questionnaire	Functional
4.Insight into BIS metrics	List of predefined metrics	Non-functional & functional
5.Use of existing management models	Knowledge items / Scope and context items / Stakeholder analysis	Functional & environmental

This table summarizes the requirements for the artefact and contribute in the deliverables set in chapter 1 and will be taken into account to be demonstrated and evaluated in chapter 7.

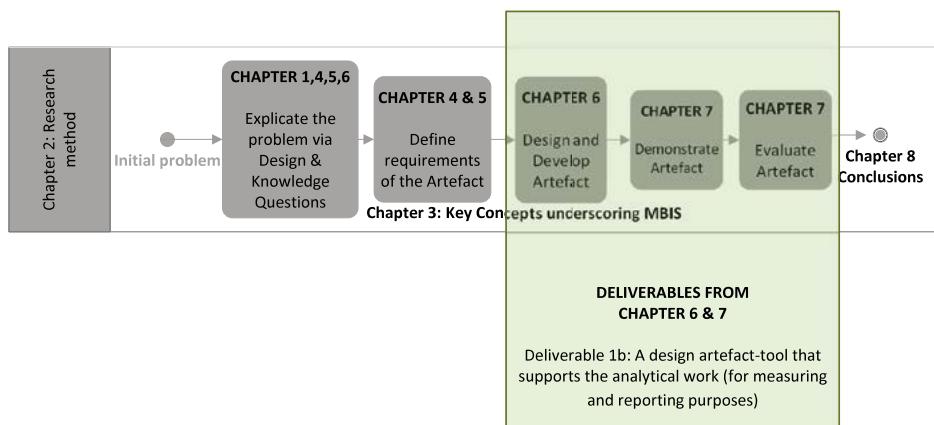


Figure 47: Deliverables from chapter 6 & 7 based upon the DSR framework of Johannesson and Persson [73].

7

DEMONSTRATING AND EVALUATING THE ARTEFACT

This chapter evaluates the way the artefact works, based on the five cases, and makes a contribution to solving practical problems that arise before, during and after the MBIS process. It also demonstrates how it solves problems experienced by stakeholders.

7.1 INTRODUCTION

Explicating the problem and designing the requirements is the initial phase of the Design Science Research approach used to establish the artefact. In the previous chapter five cases were addressed via the DSR guidelines. The previous chapter addressed the problem, potential solutions and treatment considerations that form the requirements for the artefact. In this chapter we demonstrate and evaluate the artefact. First we *demonstrate* how the requirements, which are described in Chapter 6, were implemented in the artefact. How these requirements treat problems and how the artefact functions operate and have effect. In the *evaluation step* we elaborate how the artefact was assessed in a proof-of-concept exercise during the period March - June 2011. And, after the implementation of the artefact, how it was refined, in the "design cycle", by two academics in two separate research projects. The first of these was carried out in 2013 with the objective of examining and testing the core requirements and functionalities according to the user. This was done mainly to enhance adoption by the user group. The second research project examined the gap between the current functionalities and the required functionalities in order for the artefact to function as a full "Information Security Management System" (ISMS). This last research project was performed in 2014 and 2015 and was driven by an increasing business opportunity due to regulations which require the use of a semi-automated ISMS instrument.

This chapter starts by demonstrating, based on the five cases from the previous chapter, how the previous requirements were implemented in the artefact and how the problem is treated. Finally the effect on the environment is described. This chapter deals with the last two iterations of the artefact establishment framework as described in Chapters 2 and 6 [73].

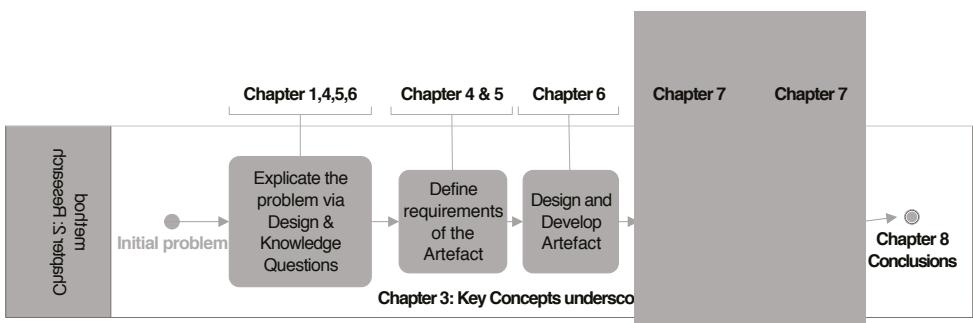


Figure 48: Research phase "demonstrating and evaluating" based on Johannesson and Perjons [73].

7.2 DEMONSTRATING THE ARTEFACT

A demonstration can be seen as a lightweight evaluation. If the artefact can address a problem in one case, it might be able to do so in other cases as well [73]. Hence the fact that a demonstration is a one-time event to demonstrate the working of the requirement we add the “evaluation process” later on in this chapter. We elaborate the choices we have made during the demonstration phase according to the “Guidelines for Demonstrating an artefact” put forward by Johannesson and Perjons.

TESTING THE MBIS ARTEFACT

All functional requirements that were required to be implemented in the artefact were subject to a change process. Initially a request for functionality was discussed with the software developer to determine the objective, impact and timelines related to the adoption of the requirements. To monitor this process an online software development tool was used to track and trace the software development process. See the Appendix for screenshots. This approach enabled me to plan enough time for the demonstration and evaluation of new requirements.

7.2.1 CASE 1: DEMONSTRATING KEY BIS MANAGEMENT INFORMATION IN THE MBIS ARTEFACT

Case	Requirement	Form
1.Key BIS management information	Dashboard on policy status, risks and evidence	Dashboard

In line with the previous Design science research approach, the guidelines from Johannessen and Perjons for demonstrating and evaluating the artefact are applied.

Case	Justify the Choice of Case Explain why the chosen case is representative of the problem and challenging enough to offer an adequate test bed	Make Clear How Much of the Artefact Is Tested. Describe the components of the artefact that are actually used in the demonstration	Make clear how and when the requirement is implemented?	Make clear how the problem is treated	Make clear the effects on stakeholders and the environment	Research strategy for artefact demonstration (Real-life, POC)
1.Key BIS management information.	The objective here is to demonstrate the working of the artefact on the item "Key BIS management information". We choose to use a dummy account with fictive data named "Nivenco" NV. This dummy account captures all the functionalities of the life version that is used by real-life organisations throughout the Netherlands.	In undermentioned visual we demonstrate the components "Key BIS management information" in the MBIS artefact. Functionalities; dashboarding, policy, risks and evidence. Over the period 2011-2015 over 50 unique accounts and over 200 assessments that make use of these components are processed.	The requirement "dashboarding" is implemented in the initial version in 2011. Policy, risk and evidence is implemented in the later versions.	The initial problem is treated by implementing the core management information for BIS, being risk, policy information and facts (evidence). Although the last one is a functionality that the user needs to activate himself it is built in in the artefact.	The effect of making use of the key BIS management information provide stakeholders in more BIS detailing on implementation of the policy's, high risks and thereby encourage the entire organisation to deliver the underlying facts (evidence).	Real-life with dummy account and dummy data.

DASH BOARDING, POLICY AND RISK

In the first screenshot we see the dashboard functionality at the initial login page. On the right below at the bottom we see the policy functionality that can be filled in in the back end of the application. This is displayed in the second screenshot (right lower box).



Figure 49: Case 1: Demonstrating dashboarding and policy.

In the screenshot below we demonstrate the risks and the indication of the risk. These are expressed in coloured arrows going up or down to indicate severity.

SECURIMETER								
Observation name	Assessment name	C	Observation	Risk description	Measure	Fix cost	Frequency	Assessment date
Vervuisterde instabiele firmware op apparatuur.	LAN Vulnerability Assessment - Technical assessment	?	De switch is gebaseerd op oude middelen van vervuisterde en onstabiele software.	De beschikbare switch kan in het begin nog wel goed werken, omdat de software stabiel is.	Het is niet verstandig om de switch bij elke update, omdat de software onstabiel is.	€ 500	Yearly	1-2-2015
Beperkt toegang matches	LAN Vulnerability Assessment - Technical assessment	?	Er wordt gebruik gemaakt van standaard administratieve account op de switches.	Uit de logiek van dienstverlening van netwerkdeuren, zijn er extra handleiding vereist.	Richt de standaard autowaterstopping in.	€ 500	Yearly	1-2-2015
Easiest logging matches aanvullijp.	LAN Vulnerability Assessment - Technical assessment	?	Er is logging aanwezig van de switches, de logging wordt periodiek opgevraagd.	De beschrijving is op dit moment nog erg afhankelijk van de interpretatie van...	De vereenvoudiging logica's worden in een systeem voor classificatie en analyse...	€ 500	Yearly	1-2-2015
Vervuisterde documentaire switches	LAN Vulnerability Assessment - Technical assessment	?	Door vervuisterde documentaire...	Door vervuisterde documentaire kan er tijdens "route choosing" extra...	Wijzen een voorwaarde aan voor het beheren van de documentaire en makkelijk gebruik.	€ 500	Yearly	1-2-2015
Vervuisterde instabiele firmware op apparatuur.	LAN Vulnerability Assessment - Technical assessment	?	De switches zijn gebaseerd op oude middelen van vervuisterde en onstabiele software...	De firewall herwerkt de logica tot het netwerk, omdat de switch niet optimaal...	Het is bij een firewall belangrijk om de altijd alle security geactiveerde update...	€ 5.000	Yearly	1-2-2015
Polices zijn niet correct.	LAN Vulnerability Assessment - Technical assessment	?	De policies die gebruikt worden voor source en destination poort en ip-adres. Tegenwoordig...	Er is een verschillende toegang tot het netwerk door een aantal...	Indien mogelijk de firewall updaten en configureren met applicatie herziening...	€ 5.000	Yearly	1-2-2015
beperkt firewall met gevoelde account	LAN Vulnerability Assessment - Technical assessment	?	Het beheer van de firewall gaat via één standaard administrator...	Er kan geen onderscheid worden gemaakt tussen verschillende medewerkers...	Authenticatie op de firewall inrichten via Radius of LDAP. Het implementeren van...	€ 500	Yearly	1-2-2015
analyse logdata op eigen initiatief beveiliger	LAN Vulnerability Assessment - Technical assessment	?	Loggen is ingeschakeld op de firewall en de verschillende logg worden periodiek ge...	Het is voor troubleshoot en analyse van incidenten of verschillende handleiding om te...	Een proces inrichten voor het controleren van de logdata en de logdata-invoeren...	€ 500	Yearly	1-2-2015
Documentaire vervuisterd	LAN Vulnerability Assessment - Technical assessment	?	Er is documentaire beschikbaar over de firewall configuratie, deze documentaire...	Door het controlen van recente documentaire kan het mogelijk zijn om...	De documentaire voor de apparatuur bewerken. Eventueel een proces inrichten voor...	€ 500	Yearly	1-2-2015
Segmentatie dmv VLAN's is op orde	LAN Vulnerability Assessment - Technical assessment	?	Het netwerk is goed gesegmenteerd door middel van VLAN's. Met verschillende...	Netwerk dat het netwerk niet goed gegeven heeft is in een ander segment...	Geen maatregel noodzakelijk.	€ 0	Yearly	1-2-2015

Figure 50: Case 1: Demonstrating the risk overview and risk indications.

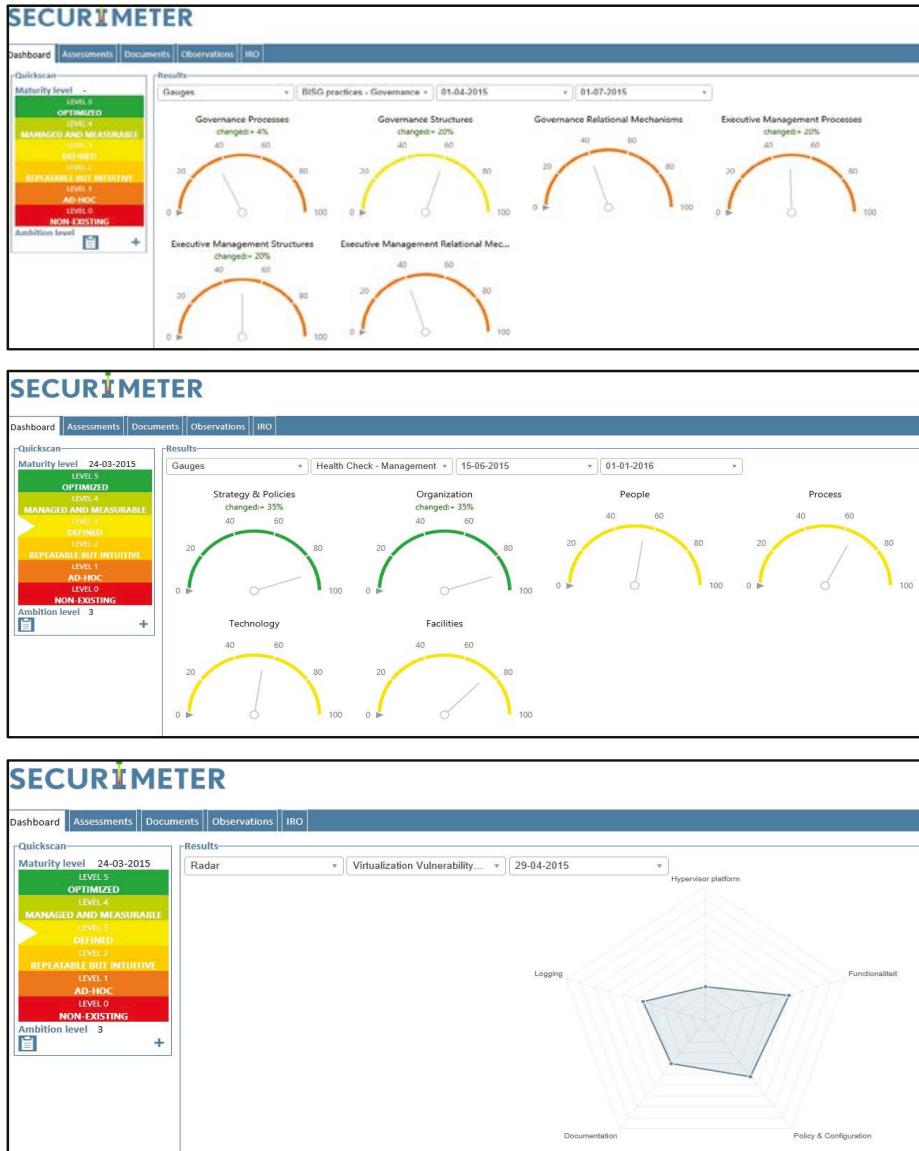


Figure 51: Case 1: Demonstrating dashboarding operational level of virtualisation vulnerabilities

Figure 52 displays the multiple dashboards on the three organisational levels (based on the Von Solms and Von Solms model). The underlying management and operational data is extracted from numerous sources as described in Chapter 1 and visualised in Figure 52 below.

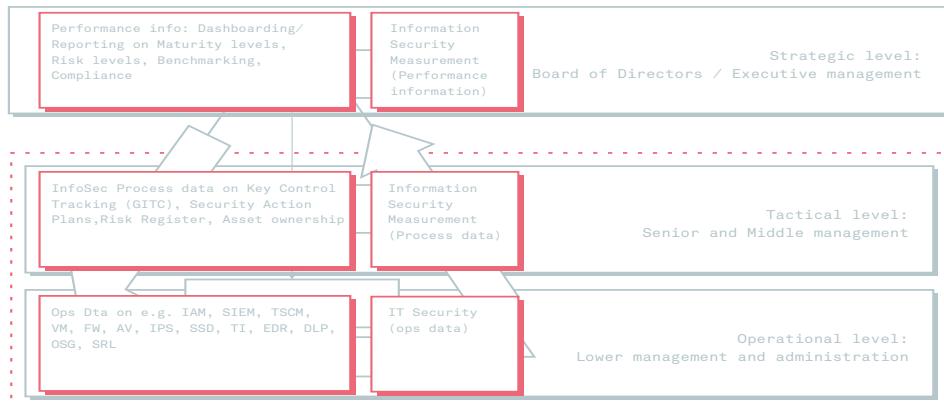


Figure 52: BIS processes and data based on Von Solms Direct, Monitor and Control Cycle [57].

The screenshot shows a web-based application interface for managing security policies:

- Company Information:**

Name	Nivenco N.V.
Branch	Government
Website	www.nivenco.nl
Number of Employees	500
Security Budget €	145000
Budget holder	Kees Janssen
Responsible person	Harry Maat
Accountable person	Piet Hein
Ambition level	3 - Defined
Include in benchmark	<input checked="" type="checkbox"/>
Risk Appetite €	
IT Dependency	High
- Address Information:**

Street	Karel Appelstraat
House number	1
Zipcode	1234 AB
City	Appeldoorn
Phone	01234567890
Fax	
Email	info@nivenco.nl
- Policy:**

Policy Applied	<input checked="" type="checkbox"/>
Policy Mandatory Compliance	ISO27001:2013
Policy Initiation Date	1-1-2014
Policy Review Date	1-1-2015
Policy Expiration Date	1-2-2016
- Remarks/Intake:**

Opmaak: Lettertype: Let... A... A...

Nivenco is actief bezig met de inrichting van Informatiebeveiliging als continu kwaliteitsproces en heeft begin 2014 een uitgebreide volwassenheidsbepaling gedaan op Informatiebeveiliging (op basis van de ISO27001 norm). Daaruit blijkt dat er een goede start is gemaakt, maar dat er ook nog stappen gemaakt moeten worden om het beoogde volwassenheidsniveau te behalen.
- Business Impact Analysis:**

A Bedreigt voortbestaan organisatie = 1.000.000
 B Aanzienlijke schade = 100.000
 C Enige schade = 10.000
 D Minimale schade = 1.000

Buttons: Save changes

Figure 53: Case 1: Demonstrating the policy setting and maintenance.

EVIDENCE-BASED

In the visual below we demonstrate that in each assessment questionnaire there is an option to upload evidence to substantiate the finding. With audits this can be made obligatory.

Figure 54: Case 1: Demonstrating the evidence collection.

7.2.2 CASE 2: DEMONSTRATING KEY BIS GOVERNANCE PRACTICES AND KSF QUESTIONNAIRE

Case	Requirement	Form
2.Key BIS governance practices and KSF	Assessment questionnaire	Functional

Case	Justify the choice of case, explain why the chosen case is representative of the problem and challenging enough to offer an adequate test bed	Make clear how much of the artefact is tested. Describe the components of the artefact that are actually used in the demonstration	Make clear how and when the requirement is implemented?	Make clear how the problem is treated	Make clear the effects on stakeholders and the environment	Research strategy for artefact demonstration (Real-life, POC)
2.Key BIS governance practices and KSF.	The objective is to incorporate the list of 20 governance practices into the artefact. The initial test case was implementation of the top 20 into the dummy account Nivenco and run several tests.	In undermentioned visual we demonstrate the components; -BISG maturity measurement, - ISO15504 NPLF scaling, -Dashboarding and reporting in the MBIS artefact. Over the period 2013-2015 > 10 unique accounts applied this artefact function. Special attention to this function was given during the Nyenrode Commissaris Cyclus in June 2014, in several master classes (Volker Wessels) in 2015	This requirement was implemented after the publication of this research at HICSS. This validation in academia legitimises to implement the list of 20 items into the test account NIVENCO.	The problem is treated by implementing the list in the artefact, share the list with the stakeholder and thereby provide inside what the current states is and what the desired status could be. One case is included I the Appendix. A company which used the list for a period of two years to treat the problem.	The initial effect is providing insight into specific knowledge items on which practices are relevant for the stakeholder (BoD). This enables boards to initiate the discussion and also enables the security professional to open up a dialogue based on corporate governance derived practices that are relevant for BIS.	Real-life artefact was used and the list was initially uploaded it the test account NIVEN-CO. After several tests by the consultants the test was promoted to the live version and applied by > 10 customers.

MANAGEMENT CONSOLE

In the first screenshot the management interface of the SecuriMeter is displayed. In this screen the superuser can create new questionnaires or assessments. He or she can create answer templates, scales, question types, and other additional functionalities that are required. In this case the NPLF scale is displayed with 10% steps.

The screenshot shows the SecuriMeter® software interface. At the top, there's a navigation bar with links for HOME, ACCOUNTS, ASSESSMENT MANAGEMENT, BENCHMARK, ADMINISTRATION, and a user profile for 'User: paul.vanvoesel'. Below the navigation bar is a sub-menu with tabs: Branches, Users, Roles, Answer templates (which is currently selected), Report templates, and ISMS data. The main content area is titled 'System Administration' and contains a table of 'Answer templates'. The table has columns for 'Id' and 'Name'. The rows show various templates like ISO15504 TECH, BIG, DNB_2013, ISO15504_NL + NVT, BIR, and several entries for 'NPLF 10% stappen'. One specific row, 'NPLF 10% stappen', is highlighted in blue. Below the table, there's a section titled 'Details' with fields for 'ID' (set to 27) and 'Name' (set to 'NPLF 10% stappen'). To the right of these details is a table with columns 'Label', 'Code', and 'Score'. This table lists Likert scale points from 'N:1%' to 'L:80%' with corresponding scores (1, 10, 20, 30, 40, 50, 60, 70, 80). At the bottom of the template list, there are buttons for '+ ADD ANSWER TEMPLATE', 'DELETE ANSWER TEMPLATE', and 'SAVE ANSWER TEMPLATE'. At the very bottom of the interface, there are status indicators for 'Development' and 'Connected', along with a 'PLUGINS' button.

Figure 55: Case 2: Demonstrating NPLF Likert score input via the management console.

ISO15504 AS A STANDARD FOR SECURITY MATURITY MEASUREMENTS

This NPLF rating refers to the ISO15504 standard. Since it is not the objective to exhaustively elaborate on maturity measurement scales but only to demonstrate the working of the artefact, we focused on demonstrating the implementation of the functionalities such as applying the NPLF scales to the questionnaires. Within the artefact numerous answering scales are defined such as open questions, closed questions, Yes/No answers, etc. The functionality of question groups and answering possibilities is displayed in the screenshot below. A detailed description on NPLF is in the Appendix.

The screenshot shows the SecuriMeter® software interface for 'Assessment Management'. At the top, there's a navigation bar with tabs for HOME, ACCOUNTS, ASSESSMENT MANAGEMENT, BENCHMARK, and ADMINISTRATION. The user is logged in as 'User: paul.van.noesel'. Below the navigation is a table titled 'Assessments' with columns for Name, Level, Version, Published, Graph on dashboard, and Visible. The table lists four entries: ISO/IEC27001:2005 controls, ISO/IEC27001:2013 controls, ISO/IEC27001:2013 controls, and BISG practices (%). A blue button '+ ADD ASSESSMENT' is located at the bottom right of the table.

Below the assessments table is a section for 'Assessment settings' with tabs for Question groups, Questiongroups and Questions, Default observations, and Account access. The 'Question groups' tab is selected, showing a list of question groups. One group is expanded, showing its details: Title: A.5. Informatiebeveiligingsbeleid, Alias: , Code: , Introduction text: , Max Score: 200. Below this, a question A.5.1.1: Beleidsregels voor informatiebeveiliging is detailed, including its title, max score (100), and a note about requiring a series of policies. It also includes fields for code, external ref, and answer types (N:1%, N:10%, P:20%).

At the bottom of the interface are buttons for 'DELETE ASSESSMENT', 'SUGGESTIONS (CSV)', 'COPY ASSESSMENT', 'PUBLISH ASSESSMENT', 'SAVE ASSESSMENT', and 'PLUGINS'. There are also status indicators for 'Development' and 'Connected'.

Figure 56: Case 2: Demonstrating the NPLF configuration via the management interface.

THE USER INTERFACE TO SELECT THE BISG MEASUREMENT

In the screenshot below the user can choose the type of assessment he/she wants to execute. On the right the date, owner, percentage of completion and numerous reporting functionalities are displayed.

SECURIMETER

[Dashboard](#) | [Assessments](#) | [Documents](#) | [Observations](#) | [HQ](#)

Taken assessments

[Clear search/filter](#)

Name	V	Taken	User	On
ISO/IEC27001:2013 controls - Business assessment	4	01-01-2016	paulvan.noest	100%
Health Check - Management	1	01-01-2016	paulvan.noest	100%
DigD (Pre Audit - 28 Richtlijnen - Operational	1	17-11-2015	paulvan.noest	4%
ISO/IEC27001:2013 controls - Business assessment	4	15-11-2015	paulvan.noest	100%
ISO/IEC27001:2013 controls - Business assessment	3	09-11-2015	paulvan.noest	0%
ISO/IEC27001:2013 controls - Business assessment	4	05-11-2015	paulvan.noest	100%
Baseline Informatiebeveiliging Rijksdienst - Business assessment	3	20-10-2015	nilla.bosker	100%
DigD (Pre Audit - 28 Richtlijnen - Operation	1	14-10-2015	paulvan.noest	0%
ISO/IEC27001:2013 controls - Business assessment	4	01-10-2015	paulvan.noest	100%
ISO/IEC27001:2013 controls - Business assessment	3	30-09-2015	paulvan.noest	0%
Health Check - Management	1	28-09-2015	paulvan.noest	0%
ITOMM - Operational	1	26-09-2015	yuri.bosker	0%
Virtualization Vulnerability Assessment - Technical assessment	3	26-09-2015	yuri.bosker	0%
Virtualization Vulnerability Assessment - Technical assessment	3	26-09-2015	yuri.bosker	0%
Wireless and Mobility Vulnerability Assessment - Technical assessment	3	25-09-2015	yuri.bosker	0%

8 10 15 25 50

Hide incomplete assessments

New assessment

[Clear search/filter](#)

Name
DigD (Pre Audit - 59 Richtlijnen
BISG practices - Governance
DigD (Pre Audit - 28 Richtlijnen - Operational
ITOMM - Operational
Health Check - Management
LAN Vulnerability Assessment - Technical assessment
Wireless and Mobility Vulnerability Assessment - Technical assessment

Figure 57: Case 2: Demonstrating the BISG assessment in the artefact.

KEY BISG IN A DASHBOARD FOR DIRECTORS AND EXECUTIVE MANAGEMENT.

In the screenshot below we demonstrate the six domains of the BISG maturity assessment that are displayed. These are: Governance processes, Structures and Relational mechanisms. Also executive management processes, structures and relational mechanisms. Each domain represents the 20 questions which are weighted via the NPLF scaling. The green percentages are the increase in maturity experienced during the period from 1-11-2014 to 1-7-2015.

7.2.3 CASE 3: DEMONSTRATING BIS MATURITY ASSESSMENT QUESTIONNAIRE

Case		Requirement	Form
	3.Key BIS management interventions	BIS maturity Assessment questionnaire	Functional
Case	Justify the Choice of Case Explain why the chosen case is representative of the problem and challenging enough to offer an adequate test bed	Make Clear How Much of the Artefact Is Tested. Describe the components of the artefact that are actually used in the demonstration	Make clear how and when the requirement is implemented? Make clear how the problem is treated Make clear the effects on stakeholders and the environment Research strategy for artefact demonstration (Real-life, POC)
3. BIS maturity assessment	According to the research results in Chapter 3 all organisations want to increase their security maturity within the coming two years but lack adequate insight how to do this. The initiated BIS maturity assessment proposed in Chapter 3 and defined in Chapter 5 as requirement was incorporated into the initial version of the artefact (date 2011). Due to the fact this was the initial requirement and functionality it was chosen to do this in a Proof of Concept.	The POC of the MBIS assessment focused on three versions. 1. The quick assessment (only six questions) this assessment has the objective to briefly highlight the main items that indicate the BIS maturity within the organisation. 2. The Basic Scan; this assessment has the objective to measure based on the twenty items raised from the qualitative research from Chapter 3. And map these items on the COBIT4.1 security maturity ladder proposed in the flow diagram in Chapter 5	The requirement was implemented in the initial version of the artefact in Q1 2011. This was done via Proof of concept under authority of the University of Utrecht in the form of a bachelor research project. The implementation was also evaluated. See next section. The problem is treated by implementing the list in the artefact, share the list with the stakeholder and thereby provide inside what the current states is and what the desired status could or should be. Five cases performed after 2011 are included in the Appendix. The initial effect is providing insight into specific knowledge items on which interventions are relevant for the stakeholder. The interventions give insight in the current status and the desired status and enables discussion between business, and security professionals. The provided list including the COBIT 4.1. measuring scale provide direct insight for the stakeholder and its environment. The POC report in the Appendix also highlights improvement effects.

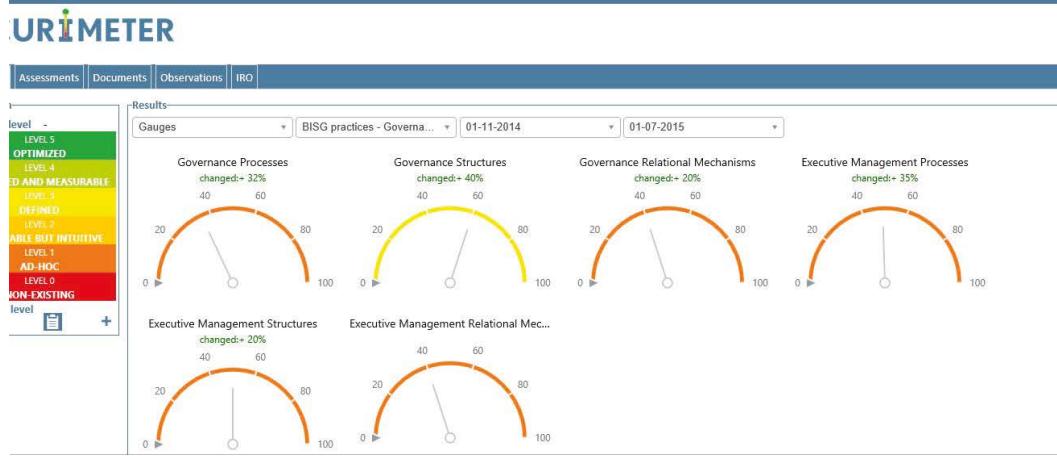


Figure 58: Case 2: Demonstrating the six domains of the BISG maturity assessment in dashboard gauges.

7.2.4 CASE 4: DEMONSTRATING METRICS IN THE MBIS ARTEFACT

Case	Requirement	Form
4.Insight into BIS metrics	List of predefined metrics	Non-functional & functional

Case	Justify the Choice of Case Explain why the chosen case is representative of the problem and challenging enough to offer an adequate test bed.	Make Clear How Much of the Artefact Is Tested. Describe the components of the artefact that are actually used in the demonstration.	Make clear how and when the requirement is implemented?	Make clear how the problem is treated.	Make clear the effects on stakeholders and the environment.	Research strategy for artefact demonstration (Real-life, POC).
4.List of predefined Metrics	The predefined requirements from this example are implemented over a longer period of time (between 2013 and 2015). Because of the number of metrics it was chosen to implement them step by step. Each requirement was proposed to the developer via the development process. Two options were possible; it was a simple change to a current functionality or it was a major structural change.	The metric component to measure and monitor the BS progression (BIS improvement) at governance level was done via: the NPLF score and is displayed via spider diagram or gauge diagram. And via the screen scope were the security organisation needs to be made explicit. The metric component to measure management is made explicit via the number of risks and the periodically increase in risk compared to the previous measurement. The effectiveness of the control and number of audit remarks. The metric component at operational level is the percentage of failed and passed penetration tests and the level of compliancy towards the security baseline.	These requirements were implemented after the performed research in 2013 and October 2014. All of the requirements were implemented via the Software development change process.	The problem of the lack of adequate metrics was mastered by the initially refinement of relevant metrics in Chapter 5. After the refinement the most relevant ones were implemented in the artefact. We have distinguished governance metrics, management metrics and operational metrics. By doing this it enables organisations to address numerous levels of the organisation in taking their responsibility and/or accountability of BIS maturity.	By distinguishing numerous levels of the organisations and their relevant metrics (according to the experts) this makes it possible to start the debate within the organisation that is responsible and accountable of delivering the data. So the side effect is the entire organisation increase in awareness on the relevance and also the responsibility to gain and maintain knowledge in order to deliver the metric data.	The requirement implementation with a large impact, for example the gauges graphs was done via a test version of the artefact. Also the Integrated risk overview which makes it possible to measure the periodically increase in the amount of risk was done via a test version. The minor changes where implemented in the real-life version and tested in the NIVENCO dummy account

DEMONSTRATING THE METRIC AT GOVERNANCE LEVEL

– Progression in establishing a BIS organisation (steering committee, CISO, CRO)

In this demonstration case we see the progression that was made during the last six months on establishing an Information Security organisation. This percentage in growth represents underlying questions the organisation needs to answer and proof in order to justify the score. In the first screenshot we demonstrate the main dashboard for the requirement “*Progression in establishing a BIS organisation*” In the second screenshot, the breakdown of the questions that needs to be answered and proofed (screenshot 3) by the organisation, is presented.

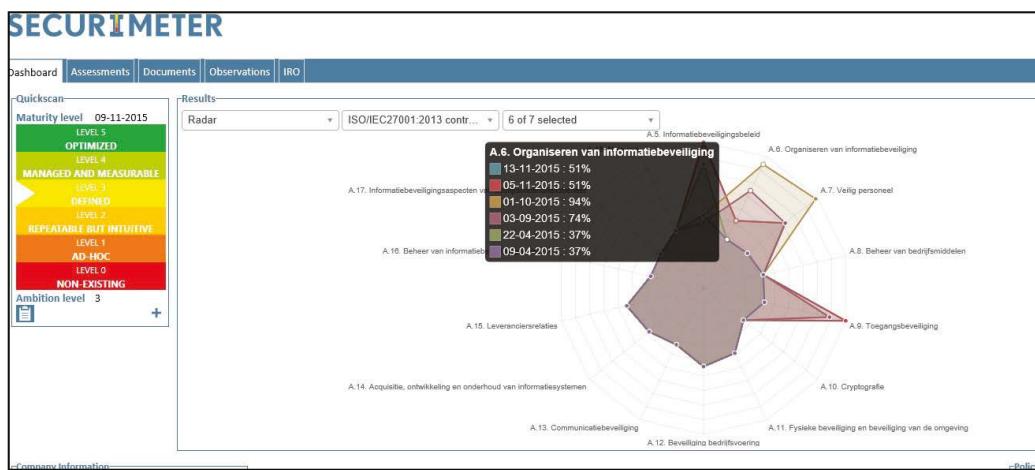


Figure 59: Case 4: Demonstrating the BIS organisation dashboard.

A.1.1. Belangen en verantwoordelijkheden bij internebeveiliging	
<input checked="" type="checkbox"/>	N/A. Internebeveiliging is niet actief
<input type="radio"/>	A.1.1. Organisatie van internebeveiliging (I/N)
<input type="radio"/>	A.1.1.1. Belangen en verantwoordelijkheden bij internebeveiliging
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:50% P:60% P:70% P:80% P:90% N/A
<input type="radio"/>	A.1.1.2. Gedrag van leden
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% N/A
<input type="radio"/>	A.1.1.3. Contact met externebeveiliging
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% P:160% N/A
<input type="radio"/>	A.1.1.4. Controle over specifieke belangengroepen
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% P:160% N/A
<input type="radio"/>	A.1.1.5. Informeertendringen in internebeveiliging
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% P:160% N/A
<input type="radio"/>	A.1.1.6. Belangen en verantwoordelijkheden bij externebeveiliging
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% N/A
<input type="radio"/>	A.1.2. Toespraken
<input checked="" type="checkbox"/>	N/A. N/A - N/A% P:20% P:40% P:60% P:80% P:100% P:120% P:140% P:160% N/A
<input type="radio"/>	A.1.3. Veiligheid en privacy (V/P)
<input type="radio"/>	A.1.4. Belangen van belanghebbenden (B/B)
<input type="radio"/>	A.1.5. Tenuiteindbaarheid (T/D/H)
<input type="radio"/>	A.1.6. Onderhoud (O/H)
<input type="radio"/>	A.1.7. Funderende beschrijving en besluitvorming (F/B/B)
<input type="radio"/>	A.1.8. Beveiliging bestuurderschap (B/B/K)
<input type="radio"/>	A.1.9. Communicatiestrategie (C/S)
<input type="radio"/>	A.1.10. Applicatie, toetsing en evaluatie van internebeveiliging (A/T/E)
<input type="radio"/>	A.1.11. Implementatie en uitvoering (I/U/E)

Figure 60: Case 4: Demonstrating Business assessment (ISO) questionnaire.

Figure 61: Case 4: Demonstrating evidencing-functionality.

- Overview of realised versus planned BIS improvements and changes per period

The screenshot below shows how the requirement "*Overview of realised versus planned BIS improvements and changes per period*" is implemented in the MBIS artefact.

In the tab "Observations" all the general observations made by the organisation are collected. The sources can vary from audits and assessments to technical tests, etc. All of these observations are then prioritised for their impact on organisations and appointed

to an owner who is delegated to mitigate the risks. Based on risk prioritisation a plan is developed which also incorporates an element of time. For example, high risks need to be mitigated prior to medium risks. In the screenshot below this prioritisation is done in graphs (dashboard) in the first column and given a priority (Must have, Should have, etc.) Also the estimated cost of the risk is included and a target date to resolve the issue. In the last two columns an indication of fixing cost as well as the due date for the next audit or assessment is given. This overview provides a planning that the security manager can use to base his or her programme on. And the financial department can use it to reserve adequate security funding.

SECURIMETER										Nivenco N.V.		
C	I	A	Priority	Estimated	Target Date	Owner	Observation status	Assessment issue	C - Risk description	Measures	Risk cost	Assessment due
✓	✓	✓	Must have	#100002	01-08-2019	ICT	Verwachting, risico's kunnen worden opgelost!	LA01 Vulnerability Assessment - Technic assessment	✓ Het risico dat een beveiliging van de infrastructuur niet voldoet.	Het is bij een beveiliging van de infrastructuur mogelijk dat de infrastructuur niet voldoet.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100003	01-08-2019	ICT	Verhoogd risico voor gegevens account	LA01 Vulnerability Assessment - Technic assessment	✓ Er is geen standaard voor de beveiliging van de gegevensaccounts.	Aanbeveling om de beveiliging van de gegevensaccounts te verbeteren.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	ICT	Uitdrukking te verhogen.	LA01 Vulnerability Assessment - Technic assessment	✓ De mogelijkheid om de beveiliging te verbeteren moet nu worden uitgedrukt.	Naar aanleiding van de beveiliging moet nu de mogelijkheid om de beveiliging te verbeteren worden toegevoegd.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	HRM	Controleerde automatisering	RS01/27/001/2019/0001 - Business assessment	✓ Van onderhoud tot automatisering kan het risico dat de beveiliging niet voldoet.	Er moet een bewijs proces & transactieën in, inc. richtlijnen, o.a. vereist.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	IT	In gebruik genomen accounts in gebruik te houden.	RS01/27/001/2019/0001 - Business assessment	✓ De mogelijkheid om de beveiliging van de gebruikte accounts te verhogen.	Een rapport moet worden gemaakt over de gebruikte accounts, omdat deze mogelijk niet voldoende zijn.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	IT	Gebruik genomen accounts in gebruik te houden.	RS01/27/001/2019/0001 - Business assessment	✓ Het mogelijk om de beveiliging van de gebruikte accounts te verhogen.	Naar aanleiding van de beveiliging moet nu de mogelijkheid om de beveiliging te verhogen worden toegevoegd.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	Onderhoud	Nietveilig beveiliging en ontbrekende gegevens	LA01 Vulnerability Assessment - Technical assessment	✓ Het mogelijk om de beveiliging van de gebruikte accounts te verhogen.	Naar aanleiding van de beveiliging moet nu de mogelijkheid om de beveiliging te verhogen worden toegevoegd.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	IT	Gebruik genomen accounts in gebruik te houden.	RS01/27/001/2019/0001 - Business assessment	✓ De beveiliging moet nu worden verhoogd.	Er moet een IT-organisatie in, dat deze voorbeeld moet volgen.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	OISD	Groot belang hiervoor en gebruik minimaal apparatuur	RS01/27/001/2019/0001 - Business assessment	✓ Dat formaat moet een toepassing hebben dat de gebruikte apparatuur kan.	Dat formaat moet een toepassing hebben dat de gebruikte apparatuur kan.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	HRM	Leg informatiebeveiliging beschrijven	RS01/27/001/2019/0001 - Business assessment	✓ De beveiliging moet nu worden verhoogd.	De beveiliging moet nu worden verhoogd.	€ 1000	14-01-2019
✓	✓	✓	Must have	#100005	01-08-2019	IT	Probleem Catalogus ontstaan.	RS01/27/001/2019/0001 - Business assessment	✓ Het risico dat de beveiliging van de gebruikte accounts niet voldoet.	Onvoldoende protocollen voor de beveiliging van de gebruikte accounts.	€ 1000	14-01-2019

Figure 62: Case 4 Demonstrating BIS improvements and periodically changes via the IRO.

MANAGEMENT

- Number of security incidents (gained via observations⁴⁴), effectiveness of security controls, development of the maturity level.

In the screenshot below we demonstrate in the left column the origins of the observations. These can be origins from self-assessments, audits, meetings, pen tests, etc. All observations are included in the artefact and labelled as risks or incidents. A risk is indicated based on the CIA triad of Confidentiality risk, Availability risk or Integrity risk. The symbols in the second column indicate the severity and provide a dashboard for management on the progression or regression of the mitigation of a specific observation (incident). In the third column the risk it can pose to the organisation is described; this can be technical, legal, personal or reputational. In the fourth column the measure (control) against the risk is defined. This is included by the risk owner on how to mitigate the risk and which appropriate control is in place. The level of appropriate controls compared to the total outstanding number of observations is an effective way to measure the effectiveness of the security programme. A disciplined team of people need to maintain the observations and extract these from the entire organisation to create the necessary exhaustive view. It is essential to have a proper

44 In Dutch noted as "bevindingen"

risk management process in place to delegate the risk to its owners as well as continuous monitoring whether deadlines for mitigation are being achieved. The sixth column represents the potential cost for the owner to fix the risk and the seventh column represents the frequency the observation is audited. The last column indicates the date the next audit or assessment is pending. This provides the risk owner with direct insight into the due date.

Assessment name	C	Observation	Risk description	Measure	Fix cost	Frequency	Assessment date
LAN Vulnerability Assessment - Technical assessment	?	De switches zijn geïnstalleerd door middel van verouderde en onstabiele so...	De beschikbaarheid kan in het geding komen, omdat de software onstabiel is.	Het is niet vereist om de switch bij elke update, die wordt uitgebracht, ook te ...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Er wordt gebruik gemaakt van standaard administratie account op de switches.	Bij afloop van dienstverband van medewerkers, zijn er extra handeling vereist om...	Richt een standaard autorisatiekoppeling in, zoals LDAP of RADIUS. Welk(e) is...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Er is logging aanwezig van de switches, de logging wordt periodiek op opgeleverd...	De beoordeling is, op dit moment, nog erg afhankelijk voor de interpretatie van...	De verzamelde logdata's voeden in een systeem voor classificatie en analyse...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	✓	Er is documentatie aanwezig, maar de aanwezig documentatie is verouderd.	Door verouderde documentatie kan er tijdens "trouble shooting" extra...	Wijst een verantwoordelijke aan voor het beheer van de documentatie en maakt gebruik...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	De firewalls zijn geïnstalleerd door middel van verouderde en onstabiele so...	De firewall beheert de toegang tot het netwerk, omdat de firewall niet optimale...	Het is bij een firewall belangrijk om de altijd alle security gereedtekening op...	€ 5.000	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	De polities zijn gebaseerd op source en destination poort en IP-adres. Tegenover...	Een aanvaller kan eenvoudig toegang verkrijgen tot het netwerk door een aanval U...	Indien mogelijk de firewall updaten en configureren met applicatie herkenning. A...	€ 5.000	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Het beheer van de firewall gaat via één standaard administrator...	Er kan geen overeenstemming worden gemaakt tussen verschillende medewerkers. Waarom...	Authenticatie op de firewall inrichten via Radius of LDAP. Het implementeren van...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Logging is ingeschakeld op de firewall en de verzamelde logs worden periodiek ge...	Het is voor troubleshooting en analyse van incidenten of storingen handig om te...	Een proces instellen voor het controleren van de logdata en de logdata inlezen...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Er is documentatie beschikbaar over de firewall configuratie, deze documentatie...	Door het ontbreken van recente documentatie kan het moeilijk zijn om troubleshoot...	De documentatie voor de apparatuur bijwerken. Eventueel een proces instellen voor...	€ 500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Het netwerk is goed gesegmenteerd door middel van VLANs. Welke segmenten...	Indien het netwerk niet goed gesegmenteerd is kan een aanval eenvoudig...	Geen maatregel noodzakelijk.	€ 0	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Alle communicatie tussen verschillende segmenten wordt afgehandeld door een star...	een virus of malware besmetting op een werkstation kan zich snel verspreiden...	Lukt de routering voor VLAN's door een firewall of switch niet uitgebreide IP...	€ 80.000	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Er is geen Intrusion Detection System of Intrusion Prevention System aanwezig...	Door het ontbreken van een IDS/IPS oplossing kunnen aanvallen op het netwerk...	Indien mogelijk IDS- & IPS functionerbaar activeren op de huidige firewall en...	€ 4.000	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Het is mogelijk om met een onbekende laptop toegang te krijgen tot het netwerk...	Het is mogelijk om met een onbekende laptop of computer aan te sluiten op het netwerk...	Een network access control oplossing instellen.	€ 2.500	Yearly	14-03-2015
LAN Vulnerability Assessment - Technical assessment	?	Het is mogelijk om op werkstations op te starten vanaf een eigen USB stick...	Het is mogelijk om beveiligingsmaatregelen te omzetten door op te starten van...	Beprek USB toegang op vaste werkkleppen tot alleen vertrouwde USB sticks. Ook...	€ 500	Yearly	14-03-2015
ISO/IEC27001:2013 controls - Business assessment	?	Er wordt geen beoordeling van het Informatie Beveiliging beleid plaats, omdat da...	Zonder reguliere evaluatie van het geldende beleid, wordt er nauwelijks betrekking...	Stel behalve IB beeld ook een reguliere evaluatie van dat beleid in, zodat...	€ 2.500	MBS	12-01-2015

Figure 63: Case 4: Demonstrating the metrics at the management level.

– Number of audit remarks

Current and new audit remarks are seen as observations and can therefore be added to the observation list as shown above. When periodically reviewing this observation overview, the user has direct insight into new audit remarks and their owners.

OPERATIONS

– Percentage of failed pen tests

Doing penetration testing on systems is a way of exploring vulnerabilities that might be exploited and might impose a security threat to the organisation. This so-called pen testing of systems can be performed in several ways. An internationally well-known method for testing is based on the OWASP top 10⁴⁵. In this research the objective used to demonstrate how the pen-test criterion, on which a thorough penetration test is based, is incorporated as a metric requirement in the artefact. It is not my intention to validate or proof the pen-test method. In the first screenshot the main categories of penetration testing criteria are laid out. In the second screenshot we see more detailing for the pen tester to perform and on which Likert scale (based on ISO15504 maturity scaling) he or she needs to score findings. By doing this

45 The Open Web Application Security Project OWASP Top 10 Privacy Risks Project provides a top 10 list for privacy risks in web applications and related countermeasures. The list uses the OECD Privacy Guidelines as a framework and can also be used to assess privacy risks associated with specific web applications.

we quantify qualitative datasets. In the third screen we see the functionality within the artefact which the user needs to attach proof to a pen-test. In this case a failed test, for example due to the lack of certain information can be reported here. In the last screenshot we can see all penetration testing results over the last year based on this penetration working method whereby all qualitative data gathering is converted into quantitative measurable data.

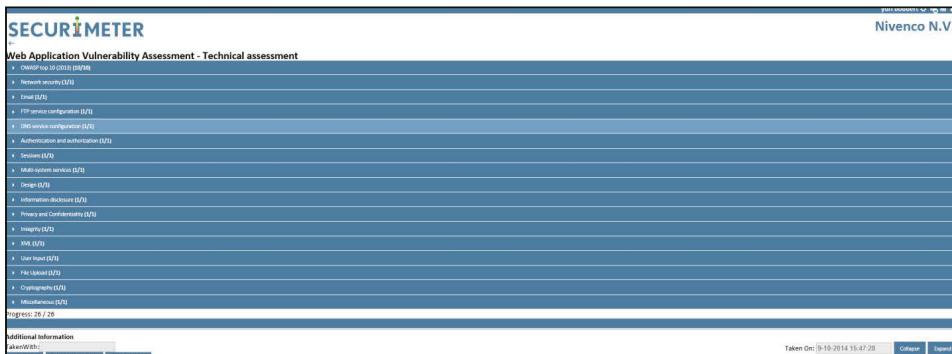


Figure 64: Case 4: Demonstrating the metrics at the operational level (pen-test scores).

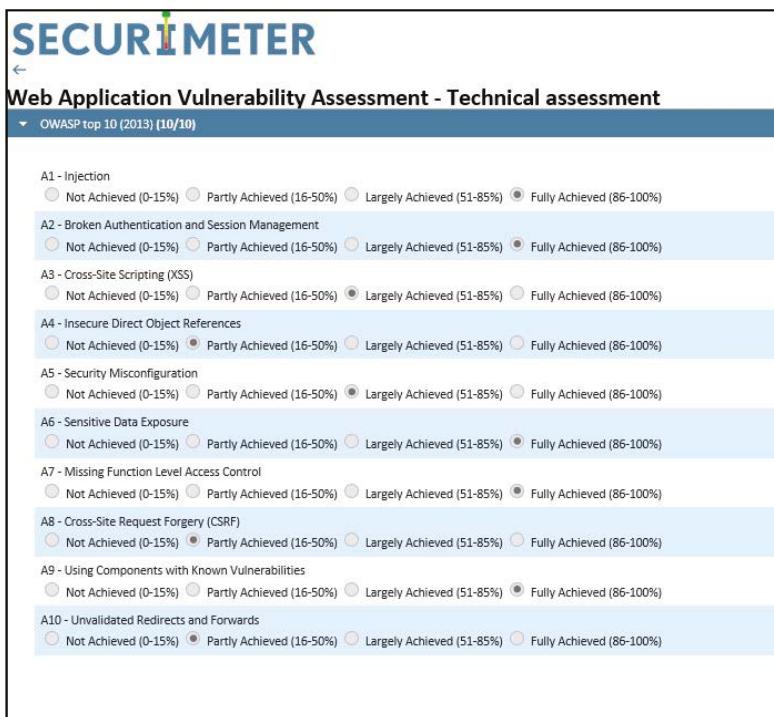


Figure 65: Case 4: Demonstrating the NPLF scales which represent pen-test score.

SECURIMETER

←

Web Application Vulnerability Assessment - Technical assessment

OWASP top 10 (2013) (10/10)

A1 - Injection

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A2 - Broken Authentication and Session Management

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A3 - Cross-Site Scripting (XSS)

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A4 - Insecure Direct Object References

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A5 - Security Misconfiguration

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A6 - Sensitive Data Exposure

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A7 - Missing Function Level Access Control

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A8 - Cross-Site Request Forgery (CSRF)

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A9 - Using Components with Known Vulnerabilities

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

A10 - Unvalidated Redirects and Forwards

Not Achieved (0-15%) Partly Achieved (16-50%) Largely Achieved (51-85%) Fully

Network security (1/1)

Email (1/1)

FTP service configuration (1/1)

Enter Proof

Assessment/Question information

Assessment: Web Application Vulnerability Assessment - Technical assessment
Question: A1 - Injection

Input Information

Input from:
Input date:

Your Proof

Input fields for entering proof, including a rich text editor toolbar.

Documents

Report Name	Actions
No data	

Figure 66: Case 4: Demonstrating evidence delivery for pen-test scores.

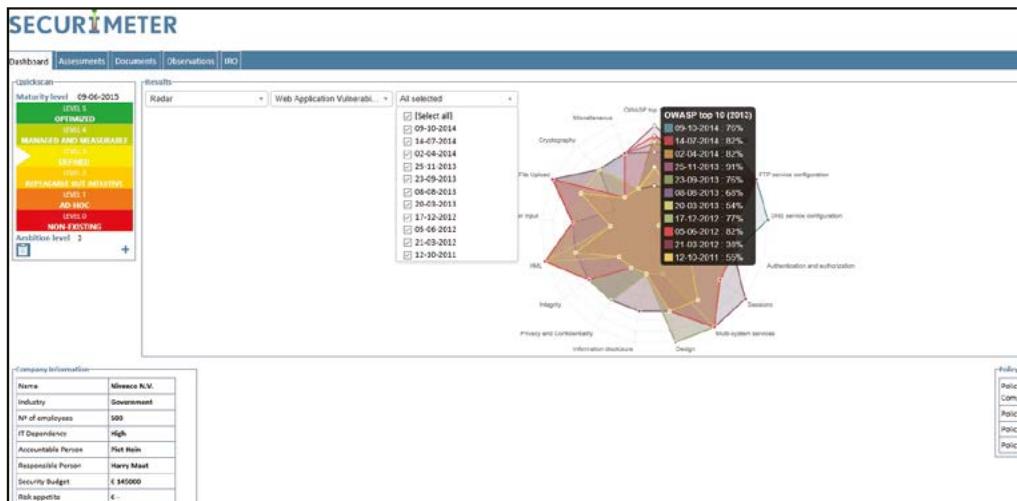


Figure 67: Case 4: Demonstrating the dashboard information of the pen test score.

7.2.5 CASE 5: DEMONSTRATING STAKEHOLDER ANALYSIS IN THE MBIS ARTEFACT

Case	Requirement	Form
5.Use of existing management models	Knowledge items / Scope and context items / Stakeholder analysis	Functional & Environmental

Case	Justify the choice of case & explain why the chosen case is representative of the problem and challenging enough to offer an adequate test bed	Make clear how much of the artefact is tested. Describe the components of the artefact that are actually used in the demonstration	Make clear how and when the requirement is implemented?	Make clear how the problem is treated	Make clear the effects on stakeholders and the environment	Research strategy for artefact demonstration (Real-life, POC)
Use of existing management models	The major problem articulated in Chapter 5 is the absence into proper scoping of the MBIS. To begin with scoping of the number of stakeholders and their expectations, requirements and needs. The problem to solve was to provide insight into the stakeholders and their dependency towards the organisation. This functionality was called the stakeholder analysis.	The stakeholder analysis was integrated into the artefact in 2013. It was performed by thoroughly decomposing the stakeholders: -Name and role (regulator, supplier, customer etc.) -Ownership in terms of who's responsible in adequately managing the stakeholder within the company, departments such as Legal, HRM, Communication, investor relations. -Affiliated risks, impact and dependencies (i.e. compliance risk, financial risks, legal risks, personal liabilities) An additional item is included to judge the contractual dependency with the stakeholder. For example, if there is a service level agreement or other form of legal agreement.	The requirement is implemented in the artefact version 4.	By explicating the entire field of digital stakeholders an organisation gains insight into their network partners. In addition, they gain insight into legal, technical dependencies. By utilising visibility this enables the discussion on how to mitigate certain legal or technical dependency risks.	By providing visibility the side-effect is the discussion among directors on the acceptance level of dependency and perhaps a certain risk appetite. This information has influence on the maturity level an organisation wants to attain and also what's needed (e.g. knowledge) to maintain a certain level. Periodically review the stakeholder analysis provides more control. Also for financial partners (Venture capitalist, Private equity, insurance and banks)	Knowledge items / Stakeholder analysis implementation in the artefact test environment

The figure below illustrates the decomposition of the artefact requirements framed as the "Stakeholder Analysis"

Titel veld:	Stakeholder - naam	Stakeholder rol -	Stakeholder eigenaar	Risico omschrijving	Kans	Afhankelijkheid				Beschreven requirements	Contract - SLA	Soort Schade -
						Business	Information	Data	Compliance			
wat komt erin	naam	Leverancier, klant, toezichthouder	afdelingen	wat is het risico	hoog, middel laag	Ja/nee: waarom	Ja/nee: waarom	Ja/nee: waarom	ja/nee: toevoeging	ja/nee	reputatie, boete enz	
Soort veld	Open veld	Dropdown: aanpasbaar per klant	Open veld	Open veld	Dropdown: hoog, middel laag	Ja/Nee en een open veld	ja/nee	Dropdown: aanpasbaar per klant				

Figure 68: Functional requirements for the stakeholder analysis.

INTEGRATED RISK OVERVIEW (IRO)

To identify associated risks which certain strategic stakeholders represent and to determine the force (static or dynamic in nature), a decomposition of the risk is made. We define:

- Risk description. This indicates what the risk is and how is it identified (as a strategic, tactical, or an operational risk). Who's the 'owner' of the risk and what is the likelihood that it will occur?
- The potential impact of the risk is indicated (based on the CIA indicators) and the impact on compliance is also indicated.

Integrating information system risks into an information risk overview (IRO) makes it easier for boards to create a holistic overview on all information-related risks.

Titel veld:	Risico omschrijving	Risico niveau	Risico eigenaar	Kans	Impact				Eisen beschreven	Soort Schade
					Confidentiality	Integrity	Availability	Compliance		
wat komt erin	wat is het risico	Strategisch, Tactisch,	afdelingen	hoog, middel laag	ja nee: wat dan	reputatie, boete enz				
Soort veld	Open veld	Dropdown: Strategisch, Tactisch, Operationeel	Dropdown: aanpasbaar per klant	Dropdown: hoog, middel laag	Ja/Nee en een open veld	Dropdown: aanpasbaar per klant				

Figure 69: Functional requirements for the Information Risk Overview.

DEFINE OWNERSHIP OF CRITICAL ASSETS

To determine ownership of critical assets it is important to set an artefact requirement that indicates this. The asset name, location, accountability and impact break down the necessary information to see if a certain force has influence on the 'crown jewels' of the organisation. Assets can be any object that contains information such as buildings, IT systems, data storage, paper files, people, etc.

Titel veld:	Impact											
	Asset	Description	Accountable	Responsible	Confidentiality	Integrity	Availability	Compliance 1	Compliance 2	Compliance 3	Compliance 4	Compliance 5
wat komt erin	Asset naam	Asset description	Person defined in Account	Person defined in Account								
	Open veld	Open veld	Dropdown: aanpasbaar per klant									
Soort veld												

Titel veld:	Naam belanghebbende	risico	omschrijving	Type maatregel	Maatregel	Eigenaar	opzet bestaan	gecontroleerd (werkung)	residual risk	Anvaard
	naam of intern(bij) wat is het business risk	risico		technisch, juridisch, contractueel, procedureel	gekoppeld aan een vraag in een assessment	naam van de eigenaar van de maatregel	ja/nee	waarde assessment	hoog middel laag, geen?	ja /nee
Soort veld	import vanuit de eerste 2 tabs(stakeholderernaam en risico eigenaar	import vanuit de eerste 2 tabs		Dropdown: Organisatorisch, Juridisch, Technisch	Hier moet een vraag aan gekoppeld kunnen worden	Dropdown: aanpasbaar per klant (contact persoon relatie)	dropdown: Ja, Nee	antwoord uit de gelinkte vraag	dropdown: Hoog, Middel, Laag, Nihil	dropdown:

Figure 70: Functional requirement setting for the asset inventory in the IRO.

Risk assurance based on an Information Security Management System (ISMS)

To align stakeholder-related risks and critical ownership with measurements that can control these risks, an assurance function is proposed as the final requirement for the artefact. With this requirement we follow the Deming Cycle of Plan, Do, Check and Act to:

- Address a certain strategic force as a stakeholder that influences our scope as well as the MBIS strategy and process (PLAN).
- Indicate the power, dependency and risk this stakeholder imposes on the organisation and therefore the extent to which it can influence the MBIS strategy and process.
- Assign the stakeholder and its risks (to critical assets) to an 'owner' in the organisation and implement appropriate actions (interventions, practices, investments, etc.) to control the risk and ensure continuity, integrity and availability (DO).
- Frequently check if all forces and related risks are mitigated by the owner (CHECK).
- Address residual risk that is not addressed by the general controlling mechanisms. Evaluate the above-mentioned steps to initiate appropriate corrective measures (ACT). Continuously involving the asset owner and stakeholder in this process increases the level of commitment [82] [259] and therefore the success of the security programme [80].

7.3 EVALUATING THE ARTEFACT

7.3.1 TREATMENT VALIDATION

In order to determine whether the requirement setting contributes to solving problems and meeting stakeholder goals, validation of treatment is required. *To validate a treatment is to justify that it would contribute to stakeholder goals when implemented in the problem context. "This is done after requirement setting and has the objective to pre-test the artefacts requirements if no real-world implementation is available to investigate whether the treatment contributes to stakeholder goals. [146]" Ideally the process of treatment validation is done*

before implementation, but sometimes this is not always the case or possible, hence the fact that in a dynamic business environment time is limiting and laboratory settings and resources have limited availability. The objective of treatment validation is also to develop a design theory, alternate alternatives or adjustments of an artefact in a certain context and to test its behaviour and outcomes once it is transferred into its intended problem context. The theory is used to predict potential outcome or formulate assumptions and/or examine alternatives.

7.3.2 EVALUATION OBJECTIVES

In this chapter we describe three forms of testing and evaluation of the artefact over a longer period of time (2011-2015), each with a different objective.

1. During the first six months of 2011 an evaluation of the initial MBIS artefact was conducted in the form of a Proof of Concept with a limited number of users with the objective of *examining how the MBIS artefact can contribute to a better BIS maturing process within the stakeholder group (mid-market companies)*.

PERIOD: Q2 2015

2. During the last 3 months of 2014 an evaluation of the current MBIS artefact version was performed by a Bachelors research student at the Haagse Hogeschool, Information Security (specialisation management). With the objective of *re-aligning the experienced business problems with the problem-solving capabilities of the artefact*.

PERIOD: Q3 2014

3. During Q2 of 2015 an evaluation of the MBIS artefact was performed in order to examine the gap between the desired functionality in the market for Information Security Management Systems (ISMS) and how the SecuriMeter can fill that gap/meet that need. This research was performed by a Bachelors research student at the Haagse Hogeschool, Information Security management direction. With the objective of *addressing the problem of organisations demanding an ISMS*.

PERIOD: H1 2011

According to the guidelines for artefact evaluation provided by Johannesson and Perjons [73] we elaborated the problem, the treatment of the problem via requirement setting, the method used to evaluate the artefact and the level of stakeholder engagement.

During the period 2011 - 2014 numerous alterations were developed within the SecuriMeter to address practical problems. We elaborate on these three evaluation cases because they were performed in a controlled environment under the supervision of a University of Applied Sciences and a direct supervisor within the organisation. During the timeframe 2011-2014 new versions of SecuriMeter were released and can be tracked via version control (youtrack). The conditions of these evaluations were therefore more constrained and under the direct authority of the supervisor. Also the official peer-review of the Bachelors thesis contributed to the reliability and validity of the evaluation work. Due to confidentiality these thesis's can be requested at the researcher.

7.3.3 PROOF OF CONCEPT TO EVALUATE THE ARTEFACT

In this research project evaluation of the artefact was initially performed in the form of a "Proof of Concept (POC)" with a limited number of key users representing the stakeholder group. The reason for a proof-of-concept setting before live testing was two-fold. In this project a real-world implementation was available and also a large number of stakeholders were enthusiastic about participating in the POC phase of the artefact design and development. Despite the large number of potential test users for the POC, we chose to have a limited number of POC users. For the Proof of Concept the key users are security managers and IT managers working in real environments and representing the real-life context. This POC was performed in the form of a Bachelor-level research project by a student at Hogeschool Utrecht (Utrecht University of Applied Sciences) and was limited in time (two months). The POC research project planning is illustrated in Table 16 in project phase 7 and 8 (taken from the original thesis):

Table 16: Planning of the evaluation of the artefact via a POC.

	PHASE	RESULT	PLANNING
1	Research existing tooling	Inventory on tooling	1-3-2010/30-6
2	Research best practices	Idea generation	1-3/30-6
3	Research combinations	Optimising tool sets	1-7/30-9
4	Functionality requirements	Functional requirements	1-7/30-9
5	Business requirements	Business requirements (company)	1-10/31-12
6	Test existing tooling	Testresults	1-10/31-12
7	Apply tooling	Apply tooling live	1-1/31-3
8	Evaluate tooling	Evaluate findings together with users	1-4/30-4
9	Redesign tooling	Process changes	1-5/30-6
10	Accept tooling	Take in production	1-7-2011

During the POC the objective was to test and evaluate the BIS maturity assessment that was set in Case 3 in Chapter 6. The questions from the proposed flow diagram were implemented in the MBIS artefact via three types of survey questionnaires:

1. *The Quick Scan.* This assessment has the objective of briefly highlighting the main items that indicate the BIS maturity within the organisation with a total of six questions that lead to a very high-level indication of maturity.
2. *The Basic Scan.* This assessment has the objective of measuring – based on the twenty items included from the qualitative research described in Chapter 4 and of mapping these items on the COBIT4.1 security maturity ladder proposed in the flow diagram in Chapter 5 see Figure 39.
3. *The Advanced Scan.* This assessment has the objective of indicating the maturity level based on ISO27001 and ISO27002.

The scope of the POC was to test these three BIS maturity assessments, generate a report

from the MBIS artefact and present it in the dashboard.

STAKEHOLDER EVALUATION

The three assessment types were evaluated with four stakeholders. The four stakeholder groups were:

1. Housing corporations
2. Insurance companies
3. Credit management and bailiff companies
4. Housing corporations.

To test whether the artefact meets the stakeholders' goals and solves the problems described in Chapter 5, the following criteria were evaluated.

Questions related to the BIS maturity assessment

Testability and recurrence. Is the audit correct and repeatable?

Is the interview time acceptable, for example for boards to give a brief indication of BIS maturity?

Questions related to the MBIS artefact tool

Is the tool exhaustive?

Is the tool (and its functionalities) understandable?

Is the tool reliable? Does it represent a valid view of relevant BIS items?

Furthermore the POC participants were asked to provide feedback on the tool as well as suggestions to improve the BIS maturity assessment.

CONCLUSIONS OF THE POC

All stakeholders formed a clear opinion of the artefact's functionalities and the BIS maturity assessment. In the table below a summary is made of their reactions. And in the Appendix there is a full report of the stakeholder evaluation. We can state that this POC gave us feedback on the fact that the MBIS tool actually contributes to solving the problem of the lack of insight into maturity levels within organisations. All participants agreed on the value of using a measurement instrument and were positive about the quick scan that managers can use to provide a high-level indication of BIS maturity. They also encourage adding the (more in-depth) advanced scan and the more technically oriented assessment to provide more evidence-based facts at the operational level of security. Important improvement suggestions are: add a validation function to proof the provided answers (audit purposes), more graph alternatives⁴⁶, make the files multilingual (the POC was in English), more in-

46 The initial dashboard function is shown in the appendix document of chapter 7 in the digital archive.

depth technical assessments and brief explanations of each question. All participants were enthusiastic about participating in a new MBIS artefact research evaluation project and would recommend the MBIS artefact to others.

An interesting finding was the fact that all participants were asked what their maturity level is at this moment and also what their desired state would be. All participants (100%) recognise the need to increase the maturity level. This underpins the earlier outcome of the research described in Chapter 4 that all organisations want to achieve a higher level of BIS than they have at the moment. This highlights the relevance of doing this research, but also the need to establish tooling to trace and proof steps during the maturing process.

REFLECTIONS ON THE POC

After this initial POC phase the tool was in development test mode for the next 7 months (in 2011) to make sure all teething problems were addressed. During 2011 numerous sessions were held with the consultants and also external expertise was acquired to evaluate and test the artefact. External expertise was acquired to better anticipate certain innovations or areas of expertise. This external view, collaboration and development in the MBIS artefact research project became a recurring process in the Design Science research "design cycle" and made it possible to solve business problems with the artefact. In the next section some important design collaborations are explained.

The POC provided us with some important alterations to the design and development of the MBIS artefact. First, we decided to establish the artefact based on agile methodologies so that each functional (not technical) test was done in the live application in the dummy account NIVENCO. Each new functionality that was initially tested successfully in the NIVENCO account was added to the "live" application so that new users could participate in real-life testing. These were usually consultants testing the new functionality with customers and asking for feedback on the spot. The artefact was therefore equipped with a feedback button for uploading direct feedback and improvement suggestions. Each month the data collected via this feedback function was analysed and discussed with the consultants and the developer. Secondly, each relevant suggestion was put on the development list (see an extract of this "youtrack" list in the appendix document that can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>).

IMPORTANT ALTERATIONS TO THE MBIS ARTEFACT AFTER THE POC PHASE

An important contribution was made by collaboration with experts in the field. Requests from the stakeholder evaluations to include more technically oriented assessments in the artefact numerous initiatives resulted in new assessments to measure the operational BIS level of organisations. Below we highlight the most important and significant contributions that were made on the operational level.

Table 17: Summary of other operational-oriented security assessments in the artefact.

INITIATION DATE	PROBLEM	COLLABORATING PARTNER	RESULT # TESTS
9-8-2011	Lack of insight into virtualisation risks (version 4)	VMware	7 assessments on version 4 and 8 assessments on version 5 per 4-7-2013**
12-8-2011	Lack of insight into Web threats	Aladdin eSafe	+20 assessments since 2011
12-8-2011	Lack of insight into firewall configuration vulnerabilities	Internal expertise and tools	+10 assessments since 2011
9-8-2011	Lack of insight into Wireless networks vulnerabilities and risks	Airtight networks, Internal expertise and tools	+5 assessments since 2011
12-8-2011	Lack in insights into LAN vulnerabilities	Internal expertise and tools	+40 assessments since 2011
5-6-2012	Lack of insight into Social media usage	Palo Alto Networks	5 assessments taken on 4-7-2013**
11-4-2013	Lack of cookie compatibility	Internal expertise	+2 assessments since 2013
11-4-2013	Lack of DigiD pre-audit requirements	NCSC	+10 assessments since 2013
9-11-2011	Lack of BYOD vulnerabilities	Internal expertise and tools	BYOD Assessment
14-6-2013	Lack of insight into web application vulnerabilities	Internal expertise and tools. HP Websinspect	+20 assessments since 2013
18-4-2013	Lack of insight into network vulnerabilities	Qualys*	+1 assessments since 2013
13-10-2013	Lack of database vulnerabilities	Oracle	+2 assessments since 2013

*Qualys reports all network vulnerabilities in an XML format. In collaboration with Qualys and a customer in the Netherlands direct import functionality was transferred from Qualys into the SecuriMeter. This functionality provides the opportunity to read all XML reports into the SecuriMeter using DLL parsing functionalities. In the Appendix the technical design and POC construction is detailed.

** See appendices for an example of evidence on how SecuriMeter keeps track of the total number of assessments.

These assessments are implemented in the artefact over a longer timeframe. In the screenshot below a fragment of all assessments are displayed.

Name
<input type="text"/>
ISO 27001:2005 Annex A EN - Management
Maturity Tree - Management
Cloud Computing - Expert
Wireless - Expert
Social Media - Expert
Virtualization - Expert
NEN 7510 2010 - Management
Awareness Assessment (klant specifiek) - -
Bring Your Own Device Assessment - Management
COBIT mapping - Management
Web Application Vulnerability Assessment - Advanced
Wireless Assessment - Operational
DigiD (Pre) Audit - 59 Richtlijnen - Operational
BISG practices - Governance
DigiD (Pre) Audit - 28 Richtlijnen - Operational
ITOMM - Operational

Figure 71: Evaluation of the artefact: List of all the BIS assessments in the artefact.

Besides these collaborations in the design cycle of the Design Science research phase of the SecuriMeter development other alterations were implemented based on feedback from the stakeholder evaluation.

- The validation function to proof the provided answers (audit purposes). This functionality is required to support the answers with proof, for example this is a regulatory demand for auditing. This functionality is described and presented in the previous section.
- More graphic alternatives were implemented during the year 2012. Besides spider diagrams bar diagrams and gauges were also introduced and implemented. The graphical interface of the SecuriMeter can facilitate al kind of graphs and visuals, depending on the audience. All graphs are also integrated into the numerous reports.
- Multilingual (the POC was in English). In the initial phase of the development the material was only in English, but due to customer requests this was amended to include Dutch as well.
- More in-depth technical assessments. This request was executed due to several initiatives as mentioned in the previous section. In the above-mentioned examples numerous collaboration initiatives were developed in the technical domain to substantiate the survey findings with operational proof. This functionality proved to be the function that was most appreciated by numerous clients. Some feedback from the field:

From MS, who is a professor in Information Security at The Hague University of Applied Sciences.

"With such a huge amount of norms and standards the CIO needs to deal with so many items, with SecuriMeter he has a simple dashboard view to monitor the most relevant items", "For the CISO the SecuriMeter can be a tool to transparently report to the board if Cyber Security Maturity is in control."

From Dr WT RE, who is a lecturer in auditing and assurance at the Free University in Amsterdam :

"Determining the level of security is a time-consuming exercise for organisations. Within Government the Baseline Information Security Government can be used for this (BIR). Organisations can facilitate this measuring process themselves by performing BIR based self-assessments to measure their own score based on the BIR. The collected evidence can be used for auditing purposes, this increases the efficiency of the auditing process. This can be even more efficient by automating parts of this self-assessment processes, for example via the SecuriMeter. This instrument facilitates evidence-based maturity self-assessments."

ARTEFACT EVALUATION ON IMPROVING THE SERVICES OFFERED

During the period 2013-2014 research was conducted by a researcher at The Hague University of Applied Sciences. The main research question was: *How can the SecuriMeter artefact be applied to improve the B-Able professional services offering?*

This research had the objective of providing answers to what kind of choices are necessary in order to improve the artefact, with the final objective of enabling better alignment with current business needs and solving practical problems. The research focused on two main users of the artefact: the customer and the consultant. The consultant basically uses the artefact to collect data, do analysis and make interpretations based on that data, and to present the outcomes in an understandable format to the customer. The customer has other requirements for the artefact. For example, Do I get answers to certain questions? E.g. does the artefact give me insight into certain gaps? Or what do I need to do in order to get to the next phase? Thus, there is a need for functionalities such as reporting and dashboards, etc.

The research method used was literature review and interviewing experts via a structured questionnaire.

I used literature review to initially position the core functionalities that contribute to better service delivery for customers. I positioned the functionalities based on pro's and con's.

Dashboarding functionality provides direct insight into the current and the desired state. It highlights the gaps that organisations need to overcome in order to reach a certain desired state of Business Information Security. This functionality provides insight for the consultant as well as the customer.

Assessments is a functionality that consultants can use to collect data from multiple sources using multiple methods. Assessments can include questionnaires, observations, data gathering, scans, etc. The main purpose of assessments for the consultants is to form a proper view of the current state of Business Information Security. For a customer it provides insights into the pain per item in the assessment and what kind of interventions they need to implement. Within assessment we distinguish two types:

1. Generic assessments are standardised according to certain norms, for example ISO27K assessments and DNB assessment. These types of standardised assessments are generic in scope and give an exhaustive view on the domains covered. Most of the time this is from a regulatory perspective (PCI DSS, HIPAA, NEN, ISO, ISF). Standardised assessments are process-oriented and therefore do not exclude predefined items that tend to be overlooked or neglected by human intellect.
2. Specific assessments tend to focus on certain domains. These can be technology domains, process domains or organisational domains. These assessments tend to gain deeper insights into certain relevant topics in certain organisations (so they are organisation-specific). Specific assessments also tend to use numerous research methods besides interview questionnaires. Usually evidence building is based on observations, documents, designs, policies, meeting notes, strategic documents, etc. The research process is therefore much more structured (i.e. better justified).

A third functionality is **programme management**. Since Business Information Security requires continuous attention, a core functionality of the artefact is programme management in order to trace improvements in BIS. This enables a structured and managed process of change throughout the organisation without too much interference from other processes. The programme management functionality is constructed by determining ontological elements such as the context of the organisations (i.e. stakeholder requirements), the scope of the programme, such as compliance with a certain regulation, increasing security maturity to a certain desired state, etc. The scope of the programme can vary depending on the objective of top management. Another element of programme management is gaining insight into the current state: collecting data via assessments in order to determine the current state based on predefined structured methods (e.g. the above-mentioned assessments). The third element is the foundation of the programme. These are fundamentals which drive the programme, such as budget allocation, management mandate, etc.

The last functionality from the literature review is **benchmarking**. This functionality provides insight into the performance of other organisations or industries.

I used interview techniques to judge the above-mentioned functionalities. The outcome is a prioritised list of functionalities according to expert opinion:

1. Reporting
2. Dashboarding
3. Assessments
4. Predefined intervention database
5. Publication
6. Programme management
7. Benchmarking
8. Document management.

Additional expert judgement was based on prioritising the functionalities for efficiency and effectiveness. The final outcome of this research provided new insights into prioritising requirements setting. In the section below I highlight the most important findings and suggested modifications. Each item is accompanied with evidence of how the refinements will be made at a later stage.

7.3.4 CONCLUSIONS ON THE ARTEFACT EVALUATION

The most important findings and recommendations are:

The **scales used** in the artefact are limited. The scales are mainly based on "yes" or "no" and "partially". This limits the consultant and the customer if questioning in more detail would

deliver nuance. It also limits a more accurate view on progression steps. I suggest the use of more standardised measurements methods such as ISO15504, which makes it possible to score each process based on percentages. This also enables the artefact programme management functionality since smaller percentage steps provide more detail on the regression or progression of the Business Information Security maturity process.

The refinement that was made to the artefact based on research findings was the adoption of ISO15504 as a process- oriented measuring scale. In the appendices are two examples: the ISO27K assessment and the Wireless and Mobility assessment. In the appendices it is explained how the assessment questions were broken down, linked to the ISO15504 percentages per maturity level and finally how they are presented in the dashboard. Also a comparison is made between the first version and the refined version.

During the interview the suggestion was made to establish a **predefined set of interventions** database. This database can be filled by users during the use of the artefact. The interview results concluded that most of the interventions are obvious and recurrent, so a "copy-paste" action from previous reports took up most of the assessment time. This is a time-consuming exercise and it can be solved by building in functionality that presents potential interventions next to each assessment question and these can then be hand-picked from a list. This enables the consultant to consider numerous alternatives to a problem. It also enables the consultant to do his or her work more efficiently; instead of copy-paste or rewriting potential advice he or she immediately generates and chooses the preferred option.

The storage of this data makes it possible to optimise, enrich, scrutinise the collected interventions and build a qualitative set of data which can be used for broader purposes, such as by scholars, publications and business consulting practices. Establishing such a qualitative set of predefined interventions enables the efficiency of the consulting process, since the consultant does not have to hand pick from multiple sources; it is simply presented in a predefined list.

Publication of the final results is done after the assessment. The current situation is that after finalising the assessment, the user can modify the results. From an auditor's perspective that is not a desired situation. The researcher made the suggestion to introduce an extra validation step. So, after the assessment report is finalised, pre-publication is possible. Then, after final approval by the customer or a principle consultant, the report can be marked as "final" and nobody can alter the data in the artefact.

The researcher also raised the **programme management** functionality as a major improvement for customers. Since the core problem is gaining insight into the exact steps needed to increase Business Information Security I introduced programme management functionalities. The first step is to determine the context and the scope of the programme. For example, which stakeholder requires a certain risk treatment within a certain period of

time? To gain proper insight into the risk we want to cover during the security programme it is necessary to gain insight into all the risks. This brings us at the first functionality of the risk register. By registering the source of the risk, for example via assessments this provides us a first impression. It is also necessary to pinpoint the impact (on confidentiality, integrity and availability) of the risk and the potential implications (i.e. legally, financially and personally). And we want to gain insight into potential solutions designed to mitigate the risk: the necessary steps an organisation needs to take in order to mitigate the risk, preferably expressed with financial data on the cost of mitigation. By quantifying the risk as well as the solution, business leaders are able to make an economic trade-off as to which risk to handle first. This insight into risk treatment is at the heart of the business case which each security professional needs to have in order to build the business case to upper management in order to start his or her Business Information Security programme. An important conclusion is the need to store most of the findings during data collection, i.e. taking assessments for audit purposes.

Document management was built in the artefact from the beginning. Based on the interviews the researcher suggested this should be taken care of by other data stores within organisations. The first reason is storage limitations within the artefact. Another reason is that most organisations are already equipped with document management systems, such as Microsoft SharePoint. So I suggested leaving in the option for attaching documents throughout the assessment process – not physically attaching documents to the tool, but rather creating cross-references to data stores. In this way users still have a central view of all relevant documents but do not burden the artefacts' storage capacity. Proper document management contributes to the efficiency and effectiveness of the services offered via the SecuriMeter artefact.

Important alterations to the MBIS artefact after the evaluation

During Q3 2014 most of the alterations were implemented in the artefact. We list the most relevant ones.

The **used scales** are standardised towards the ISO15504 range of maturity assessment. The numerous screenshots in this chapter demonstrate the working of these scales.

A **predefined set of interventions** is implemented with the ISO27001:2013 control assessment. Within the Business assessments al predefined assessments are available via the button Observations and then the button Select predefined:

Observations

[Back to List](#) [Select Predefined](#)

Observation name	<input type="text" value="ISO/IEC27001:2013 controls - Business assessment"/>
Assessment name	<input type="text" value="4"/>
Assessment version	<input type="text" value="A.5. Informatiebeveiligingsbeleid"/>
Domain	<input type="text"/>
Risk classification	<input type="text"/>
Frequency	<input type="text"/>
Fix cost	<input type="text"/>
Observation	<input type="button" value="X"/> <input type="button" value="D"/> <input type="button" value="U"/> <input type="button" value="S"/> <input type="button" value="I"/> <input type="button" value="B"/> <input type="button" value="F"/> <input type="button" value="M"/> <input type="button" value="C"/> <input type="button" value="P"/> <input type="button" value="L"/> <input type="button" value="R"/> <input type="button" value="E"/> <input type="button" value="N"/> <input type="button" value="G"/> <input type="button" value="H"/> <input type="button" value="J"/> <input type="button" value="K"/> <input type="button" value="O"/> <input type="button" value="V"/>

Figure 72: Artefact alterations after the evaluation; a predefined set of interventions.

Publication of the final results is now restricted. After finalisation of the assessment it is no longer possible to make any alterations unless the user has certain rights. Alterations afterwards are logged and a warning screen pops up. See screenshot.

		Date	User	Completed	Actions
2012013 control - Business assessment		11-11-2016	Paul van Nistelrooij	100%	View Edit Delete
Formulierevaluatie Nederlandse Gemeenten - Business assessment	Index	11-11-2016	paul.van.nistelrooij	100%	View Edit Delete
Op 16 - Governance		10-11-2016	Paul van Nistelrooij	0%	View Edit Delete
Formulierevaluatie Rijksoverheid - Business assessment		18-11-2016	Nikolaus Hartmann	0%	View Edit Delete
Validity Assessment - Technical assessment	Index	14-04-2016	Hans Meijer	100%	View Edit Delete
2012013 control - Business assessment		12-04-2016	Paul van Nistelrooij	100%	View Edit Delete
Validity Assessment - Technical assessment		14-02-2016	Hans Meijer	100%	View Edit Delete
2012013 control - Business assessment		12-01-2016	Hans Meijer	100%	View Edit Delete

Figure 73: Changes after the evaluation, warning screen for locking and unlocking assessment results.

Document store: Categorised list of documents that can be stored in the artefact or be linked to a document management or file sharing system (e.g. a SharePoint portal)

SECURIMETER					Nivenco N.V.
Category	Name	Remark	Classification	Created	Actions
+ Category: Informatie	Nationaal Cyber Security Center		Public	11-5-2015 17:08:42	
+ Category: Informatiebeveiligingsbeleid	Nivenco N.V. - Informatiebeveiligingsbeleid v1.0.pdf	Versie 1.0 uit mei 2014	Internal	10-12-2014 10:34:43	
+ Category: ISO27001 assessments	Nivenco N.V.- ISO27001-2013 assessment v1.1 20150412	Versie 1.1 uit April 2015	Confidential	28-4-2015 15:32:35	
	Nivenco N.V. - ISO27001-2013 assessment v1.1 20150112	Versie 1.1 uit Januari 2015	Confidential	28-4-2015 15:31:46	
	Nivenco N.V. - Toegangsbewijsbeleid v1.0.pdf	Versie 1.0 uit April 2014	Confidential	23-4-2015 13:19:05	
	Nivenco N.V. - Belied Classificatie Informatie v1.0.pdf	Versie 1.0 uit Maart 2014	Confidential	23-4-2015 13:18:12	
	Nivenco N.V. - Belied Beelding of wijziging	Versie 1.0 uit Februar 2014	Confidential	23-4-2015 13:17:16	

Figure 74: Artefact alterations after the evaluation: Document management system.

Another important alteration that was made in version 5 was introducing the Integrated Risk Overview (IRO). An observation needs to be manually forced into the IRO. Therefore users need to deliberate choose the option which observation they perceive as a business risk and treat it accordingly. User must deliberately choose the function "analysed" (column A)

	Measure	Fix cost	Frequency	Assessment date	A	
et geding nstabiel is.	Het is niet vereist om de switch bij elke update, die wordt uitgebracht, ook te ...	€ 500	Yearly	14-03-2015		
van andeling	Richt een standaard autorisatiekoppeling in, zoals LDAP of RADIUS. Wellicht is e...	€ 500	Yearly	14-03-2015		
ment, nog pretatief	De verzamelde logdata's voeden in een systeem voor classificatie en analyse,....	€ 500	Yearly	14-03-2015		
tie kan er tra t...	Wijst een verantwoordelijke aan voor het beheer van de documentatie en maak gebruik...	€ 500	Yearly	14-03-2015		
ang tot het et	Het is bij een firewall belangrijk om de altijd alle security gerelateerde updat...	€ 5.000	Yearly	14-03-2015		
toegang	Indien mogelijk de firewall updaten en	€ 5.000	Yearly	14-03-2015		

Figure 75: Evaluating the artefact; enforcement of treatment of risks.

For the observation that was promoted to a business risk a certain number of criteria need to be met in the artefact. This way the observation and all changes are logged and monitored. Changed events will be underlined in the logging and cannot be deleted or changed afterwards. This fits in with evidence-based auditing requirements.

Assessment Date	30-01-2015
Attached documents	No attached documents
IRO - Analysis	
Estimated business risk	<input type="text" value="High"/>
Impacts confidentiality	<input type="checkbox"/>
Impacts integrity	<input type="checkbox"/>
Impacts Availability	<input checked="" type="checkbox"/>
Priority	<input type="text" value="Could-Have"/>
Owner	<input type="text" value="ICT"/>
Estimated risk cost	<input type="text" value="12253,00"/>
TargetDate	<input type="text" value="1-6-2015 00:00:00"/>
Progress	<input type="text" value="Normal"/>
Analyzed (Shows this item in the IRO analysis screen)	<input checked="" type="checkbox"/>
<div style="border: 1px solid black; padding: 5px;"> <p>15-06-2015 14:09 by Paul van Noesel High A CouldHave ICT 12253,00 01-06-2015 Normal Analyzed Weer hoog</p> <p>15-06-2015 14:06 by Paul van Noesel Low A CouldHave ICT 12253,00 01-06-2015 Normal Analyzed Alles aangepast</p> <p>15-06-2015 14:05 by Paul van Noesel High CIA ShouldHave Directie - 01-04-2015 None Analyzed Availability toch belangrijk</p> <p>15-06-2015 14:01 by Paul van Noesel High CI ShouldHave Directie - 01-04-2015 None Analyzed</p> </div>	

Figure 76: Evaluation: Artefact alteration after evaluations on IRO indicators.

ARTEFACT EVALUATION ON MATCHING THE ISMS REQUIREMENTS

In Q2 of the year 2015 a Bachelors student at The Hague University of Applied Sciences did research on the main gaps between the SecuriMeter artefact and an Information Security Management System (ISMS). This research was required to examine the differences between functionalities already in the SecuriMeter and the additional functionalities needed in order for the SecuriMeter to function as an ISMS system. The method used was a survey of ISMS literature and interviews with consultants, customers and partners (stakeholders). In the second research phase, a GAP analysis was performed in order to determine the IST (current) and the SOLL (desired) situation, purely from the perspective of ISMS requirements. This Bachelors thesis is available on request.

The main function of the MBIS artefact SecuriMeter is to measure the organisation and its process of becoming more mature in order to maintain this as a continuous process.

The main function of an ISMS is a systematic approach to initiating the plan, do, check and act cycle on adequate security controls. ISMS can be implemented in a system in order to continuous monitor the controls within the ISMS framework. The most common used digital form of an ISMS is Microsoft Excel or SharePoint.

ISO27001 is the Information Security Management System Framework which encompasses the ISO27002 controls. The 27001 and 27002 are part of the broader family of standards that help organisations with the security of critical assets.

The main contributions of this research project on the evaluation of the MBIS artefact are five key suggestions for improvements. In the Appendix (Evaluation of the artefact - five suggestions for improvement) the screenshots are added, taken from the Bachelors thesis.

1. **Observation registration** per question in the questionnaire. This used to be per sub-category of questions. So it was unclear which observation was linked with which questions.
2. **Filtering functionality** per domain and question. This enables the security manager to categorise certain observations and their required actions. By filtering per item and owner, accountability of the risk becomes transparent.
3. Date and time "**check**" **functionality**. This makes it possible to track and trace the planning and deadlines of certain predefined action items in terms of expiration. In order to function as full ISMS continuous reminders of the PDCA cycle actions is required. In the screenshot in the appendix suggestions are made on how to alter the MBIS artefact in order for it to function like an ISMS tool.
4. **Correction activity prior to a new assessment**. This makes it possible to set a certain action item before a certain assessment or audit takes place.
5. **Transfer observations, proof and action items on to a new assessment**. This enables us to compare multiple assessment outcomes and observe if a certain progression is made compared to previous assessments. In the screenshot in the appendix is visualised how this functionality can be incorporated in the artefact.

7.4 DISCUSSION ON DEMONSTRATING AND EVALUATING THE MBIS ARTEFACT

In the previous sections we present some examples of the cycle involved in demonstrating and refining the artefact. The three research projects described in the beginning of this section (Evaluating the artefact) had the objective of re-evaluating the MBIS artefact and contributing to its relevance by making the MBIS artefact more aligned with current business problems that are experienced by stakeholders. The first research was performed to gain a broad overview of requirement evaluation with a small set of customers. A proof of concept, in combination with interviews, provided me with a more in-depth view of perceptions and suggestions from the target group (5 customers), in order to further develop the artefact during the design cycle.

The second evaluation focused on prioritising functionalities already implemented in the artefact. The objective here was to rigorously examine, via literature review and experts' opinions, the existing functionalities for market fitness and relevance to the environment. The outcome of this research is to prioritise requirements from a consultant's and customer perspective which was entirely implemented as functionalities within the artefact. The collective knowledge of literature and relevance (consultants) provided a prioritised set of functionalities.

The third research process was performed with the objective of filling the gaps towards creating a working Information Security Management System, a management system which enables consultants as well as customers to get a continuous process and closed loop between risk, security, compliance and assurance. The secondary focus of this research was the business opportunity for selling the artefact as an ISMS system.

Besides these three examples of fairly conditioned evaluations, the consultants and users also provided feedback on the artefact. This feedback was collected in an integral overview. The artefact evaluation and feedback form is included in the appendix which can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>.

7.4.1 EVALUATION OF THE KNOWLEDGE ITEMS

Besides the functional requirements designed and presented in the previous chapters, various knowledge items were also raised during the many research projects. We elaborate Case 5 from Chapter 5 and 6. This concerned the use of Michael Porter's model for strategy formulation by security officers. And, whether this management model helps the security manager by a) enabling this with a better understanding of external forces that he/she needs to reckon with, and b) gets his or her message across due to the use of existing management models (and not complex jargon). The evaluation of these knowledge items was performed on 10 September 2015 at Erasmus University in Rotterdam. The session raised important and interesting results. The audience consisted of IT managers, CIOs and security professionals. Through the use of GSS facilitating software, 28 respondents participated in this small research project/lecture. The main conclusions from the session are:

- It became very obvious that security should be a boardroom topic. All respondents disagreed with the proposition "it is totally irrelevant whether the board finds security important."
- According to the respondents, current management models can be re-used. The undermentioned model from Harvard professor Michael Porter (Five Forces model) can be used by the Chief Information Security Officer to determine the strategic forces of influence and advise board members.
- Knowledge is not a limitation for a board member, but awareness is. This statement requires some additional explanation since knowledge is content specific and awareness is knowledge of existence. Awareness is about knowing what knowledge you have or don't have. In this case having basic awareness on certain security and risk-related topics are addressed 3 out of 12 times by the GSS participants. Knowledge was mentioned 2 times out of 12 by the participants when they were asked about the critical success factors of BIS adoption. One of the participants raised that Knowledge is not a limitation for BoD but awareness is. Therefore, in-depth knowledge is not required, but a minimum level of security awareness by boards is, in order to take effect. Source: step 6 of the GSS session "voting of the propositions".
- All participants rank "Security on the board agenda" as the most critical success factor for effectively adopting security as a boardroom topic. The participants raised the fact that it

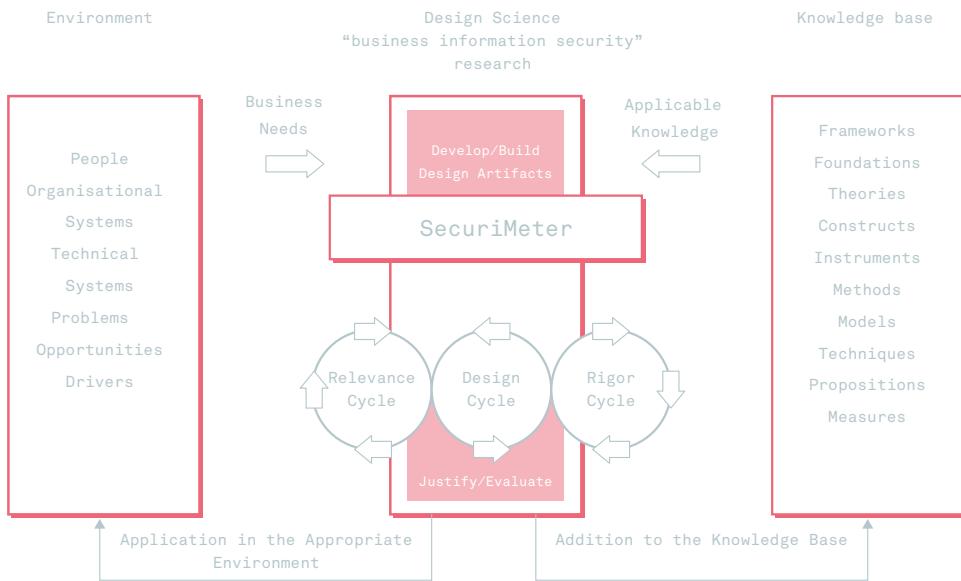


Figure 77: Design Science Research framework for transferring knowledge through the DSR artefact.

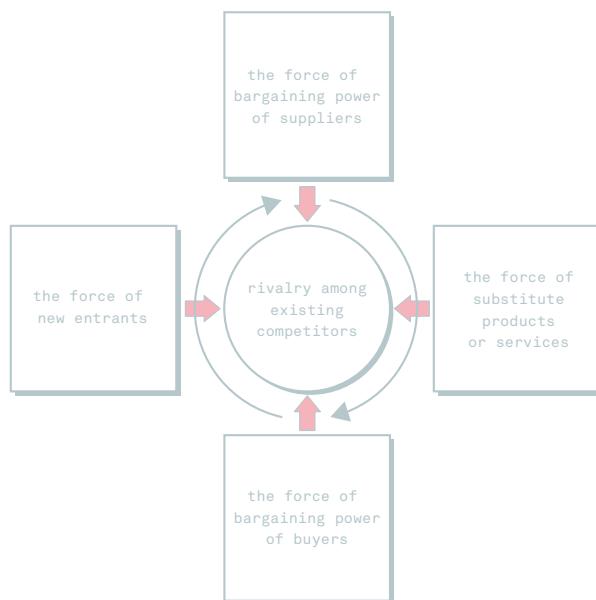


Figure 78: Michael Porter five forces model.

does not stop with putting it on the agenda. Board members should also act on it and behave accordingly.

Other critical success factors that were mentioned are: knowledge, innovation, awareness, knowledge through gaming and accountability. Most of these critical success factors were also raised by the experts in Chapter 3 and 4.

After a discussion between the participants it became clear that most of the effects can be found in the softer factors such as “tone at the top” and other non-instrumental elements.

The entire research report is included in the Appendix.

Some interesting feedback was received from numerous participants on the method used (meeting software) as well as the knowledge gained in relation to new insights and ideas.

AW from Oracle: *“Through the used method we immediately had direct contact with each other and were able to work as we have had worked with each other years before. I really enjoyed participating and debating to establish concrete results.”*

JL from Erasmus University: *“I wish we had had more time to discuss underlying thoughts in-depth. The group discussion is always very valuable in these types of research methods and I wish you could challenge the participants to express their thoughts instead of using predefined lists.”*

7.4.2 CONTRIBUTION TO THE ARTEFACT EVALUATION OBJECTIVES

In order to determine to what extent an artefact is effective for solving the explicated problem it is important to set objectives for the evaluation. This was done in the first section of Chapter 7.3.2. We hereby elaborate, based on the evaluation method of Johannesson and Perjons [73], per objective how this was met:

Objective 1. Examine how the MBIS artefact can contribute to a better BIS maturing process within the stakeholder group (mid-market companies).

This objective was met by developing a working instrument that can measure BIS maturity on multiple levels (governance, management and operations) as well as from multiple perspectives such as those of technology, processes and people. The metrics provided can function as measurement variables which each organisation can preselect.

Objective 2: Re-align the experienced business problems with the problem-solving capabilities of the artefact.

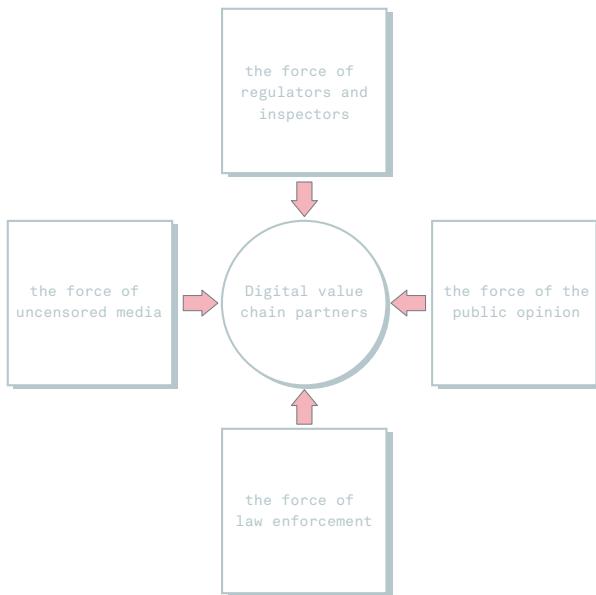


Figure 79: Michael Porter Five Forces model according to the research data from case 5.

This objective was met due to the fact that I handed over a prioritised set of relevant functions that were required at that time from different perspectives: those of customers and consultants, thus directly contributing to solving the problem at hand. The rigorously validated functionality list also makes it possible to strip the artefact from non-relevant requirements that were built in along the way and did not undergo a rigorously development process prior to implementation.

Objective 3: Address the problem of organisations demanding an ISMS. And examine what else the SecuriMeter needs to function as an ISMS.

This objective was met due to the five suggestions I made. These suggestions cross the GAP between the current and desired situations, the current situation being the SecuriMeter with its current functionalities and the desired situation being the SecuriMeter with full ISMS functionalities.

7.4.3 COMPARISON OF THE ARTEFACT

INTRODUCTION

In this stage of the research project the SecuriMeter artefact is demonstrated and evaluated based on its own capabilities and requirements set via the previous chapters. An artefact comparison against an existing other artefact can bring additional insights on the working and the artefacts' positioning compared to other tools. It can also support the future development process of the artefact. In agreement with the manuscript commission an objective comparison between SecuriMeter and a similar security measurement and reporting tool is proposed. The manuscript commission and then researcher agreed to compare the SecuriMeter Artefact with the tool of the Information Security Forum (ISF), "The ISF Accelerator". By comparing both tools based on the ENISA criteria (1)⁴⁷, these criteria were set based on an extensive examination by ENISA into Information Security and Risk management tooling. According to the manuscript commission these criteria are sufficient for the required comparison and will contribute the research project in its' academic contribution. In agreement with the promotors and the manuscript commission it was decided that in addition to the ENISA criteria, both tools also needed to be compared based on the scientific claim (e.g. functionalities) that were derived from this research work and as presented in this thesis (2)⁴⁸. Since this thesis is based on Design Science Research, and the control over progress and effects within DSR are typically at the hands of the person designing, i.e., the researcher, the comparison needs to be objective, thus without interference of the researcher, and repeatable. Important note is that during the comparison study no new release of the artefact was made, thus the entire study was executed on the same version.

I have selected GSS as a method for this qualitative comparison of tooling since GSS is also proposed in the entire thesis as a research method to gain a deeper understanding of the topic and to record intermediate steps. GSS is a research method that can use multiple iterations, with or without group interactions [107] and all steps, scores and arguments are recorded in the GSS software to assure objectivity, controllability, repeatability. With this in mind the following research approach is proposed.

RESEARCH APPROACH FOR THE ARTEFACT COMPARISON

In chapter 2 potential research risks are addressed. The risks of objectivity, controllability, repeatability and generalisability are taken into consideration during this comparison study. Therefor the following objective criteria and controllable steps are embedded. The criteria that form a "Frame of Reference" are:

- 1. ENISA Criteria, and
- 2. Additional criteria derived from the deliverables in this PhD research project:

⁴⁷ European Network and Information Security Association predefined "security and risk tool" criteria. The criteria can be found on <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/template>

⁴⁸ The thesis presents core functionalities within the SecuriMeter artefact which are derived from the Design Science Research work

The following controllable research steps and goals are proposed;

FIRST STEP:

- The researcher submits the criteria proposed by the commission, being ENISA criteria, and the presented functionalities of the SecuriMeter artefact to the promotor. The entire list of criteria is also attached in the appendices. The goal is to have clear predefined criteria which can be compared in the next steps.

After this the 100+ criteria are delivered to co-promotor professor Mulder who processed the criteria in an online survey tool so a group of experts can prioritize the criteria on relevance for comparison. Before submitting it in final version to the experts Mulder requested a group of nine people to test the set-up, in this pre-test the criteria, the listing and the online tooling. This is called step 1a. According to Recker [77] Page 78, *"a pre-test is a tryout, and its purpose is to help produce a survey form that is more usable and reliable. Pre-testing helps refine the instrument and ensure executability of the survey"*. Recker describes on page 80 of his book to perform an instrument pre-test three objectives to pursue when doing pre-tests of survey instruments:

- Evaluate the authenticity of the questions,
- Evaluate the survey interface and layout, and
- Establish validity and reliability of the survey instrument.

Table 18: List of participant characteristics of the online survey test step 1a.

PARTICIPANT	ROLE	INDUSTRY	SUBMITTED
1	Project manager security	Financial Services	Y
2	Director	HR Services	Y
3	Director	Educational Services	N
4	Manager SOC	Telecom	Y
5	Manager Call Center	Financial Services	Y
6	Director	Risk & Security company	Y
7	Security Architect	Government	Y
8	Teacher Security	Educational Services	Y
9	Security Officer	Government	Y
10	Project manager security	Airport / Aviation	Y

After the test feedback is gained to improve the tool, listing and prepare the real sessions. Also potential ambiguous terms or vague items can be detected and anticipated on. After this a large heterogeneous group from multiple business domains can score the provided criteria based on relevance for comparison and on the validity for the risk and security field. In this initial step the participants are not able to influence each other [117] nor are they influenced

by the session operator professor Mulder. This group is referred to as 1b in the appendix "Research approach tool comparison".

Table 19: Participant characteristics in the comparison study step 1b.

PARTICIPANT	ROLE	INDUSTRY	SUBMITTED ONLINE	PRESENT AT 6 JULY SESSION
1	CISO	Media	Y	N
2	CISO	Financial Services	Y	N
3	Software Security specialist	Software testing	Y	Y
4	Manager	Accountancy	Y	Y
5	Consultant	Security Services	Y	Y
6	Consultant	Security advisory	Y	N
7	Director / Professor	Research Institute	Y	Y
8	Partner at consulting firm	Security and Risk advisory	Y	Y
9	Director EMEA	Security and Risk advisory	Y	N
10	Director Security Services	Security and Risk advisory	Y	N
11	Consultant	Security and Risk advisory	Y	Y
12	Auditor	Financial Services	Y	N
13	Information Security Officer	Government	Y	Y
14	Auditor	Financial Services / Auditing	Y	N
15	Consultant in Education	Educational services	Y	N

With this step all scores are recorded per participant and analytical motivations are submitted in the system. This is to assure the objectivity, controllability and repeatability during and after the research project.

An additional GSS session is held based on the online pre-submitted data. This so called "Relay Group method" increases the productivity of the group and enables a double loop learning [148] which increase the quality of the outcome [297]. To address the large deviations between the individual scores and to discuss this in the group a better qualified core set of criteria is established which has been validated by experts from the field. Also a prioritisation of all the criteria is done based on the relevance for a comparison study.

All steps, scores and arguments are submitted in the GSS system to assure the objectivity, controllability and repeatability. The sessions are moderated by an experienced session moderator, which is required according to the ground rules of group moderation published by Hengst [115] and addressed in multiple other publications [298], [112], [149].

The objective of this first step is to selectively narrow down the 100+ list of criteria to eventually establish a core set of criteria that can be considered relevant according to experts

opinion and to do a further thorough comparison analysis on in the next steps.

SECOND STEP

The second step is to record the two tools in a video demonstration on their performance with regard to the selected criteria.

1. SecuriMeter tool is presented in a demo to present the previous derived criteria (origin; 1 (ENISA) and 2 (Additional)). This demonstration is recorded on film to assure objectivity, controllability, repeatability.
2. ISF "Accelerator" tool is presented in a demo to present the previous derived criteria (origin; 1 (ENISA) and 2 (Additional)). This demonstration is recorded on film to assure objectivity, controllability and repeatability.

The objective of this second step is to deliver two tool demonstrations on video about the core functionalities/criteria of both tools.

THIRD STEP

In this third step eleven other participants from a heterogeneous group participate in a GSS session which will be moderated by co-promotor professor Mulder. A predefined agenda is set and shared prior to the meeting so the participants can individually prepare the GSS session. The GSS session is introduced by the two video demonstrations of the artefacts. According to Recker video films increase the credibility (e.g. internal validity) (page 94), this method was chosen to assure the objectivity and controllability of the comparison study [77]. All 11 participants are asked to compare the presented functionalities and score the functionalities. All steps, scores and arguments are recorded in the GSS system to assure the objectivity, controllability and repeatability of the research. The objective here is to deliver an in-depth analysis on the predefined selected criteria and an analysis on the deviations given by the expert respondents.

Table 20: List of participant's characteristics of the GSS expert panel held on 10th August 2017 (step 3).

PARTICIPANT	TITLE	ROLE	INDUSTRY	INVITED	PRESENT AT 10 TH AUG
1	Dr.	Security Consultant	Information Security Services	Y	Y
2	Drs., MA	Advisor	Government	Y	Y
3	Dr. RE	Auditor/lecturer	Government	Y	Y
4	MSc CISA	Consultant	Information Security Services	Y	Y
8	Drs., CISM, CISA	Auditor / ISACA Chair	Financial Services	Y	Y
6	MSc, RE	Auditor	Financial Services	Y	Y
7	Prof. Dr. ir.	Professor	Education	Y	Y
8	MSc	Consultant	Security Services	Y	Y
9	MSc MISM	Information Security Officer	Transportation	Y	Y
10	BC, RE	Auditor	Financial Services	Y	Y
11	MSc	Information Security Officer	Government	Y	Y

THE FINAL DELIVERABLES OF THESE 3 STEPS ARE:

- Clearly defined criteria for the tool comparison.
- Two demonstrations of both tools recorded on film.
- An in-depth comparison analysis of both tools based on predefined criteria.

ASSURING THE ACADEMIC RIGOUR DURING THE COMPARISON STUDY

While constructing an artefact based on interpretive qualitative methods, such as the applied DSR, requires the researcher to demonstrate sufficient objectivity and academic rigour. To demonstrate this rigour, and the risks associated with interpretivist research as addressed in chapter 2, an additional comparison study was executed that caters the principles of Replicability, Independence, Precision and Falsification set by Recker [77];

Replicability refers to the term to which extent research procedures are repeatable and would lead to similar outcome. Independence (reliability) refers to the level if other individuals would reach the same conclusions as the researcher based on the same data. Recker states; "*If dependability can be demonstrated, it is similar to reliability in that it is demonstrated that measures provide consistently similar results*" [77].

In the case of this comparison study a predefined frame of reference for the comparison criteria, is used in the form, of the ENISA criteria, combined with the core functionalities derived from this research project. This frame of reference, together with the approach

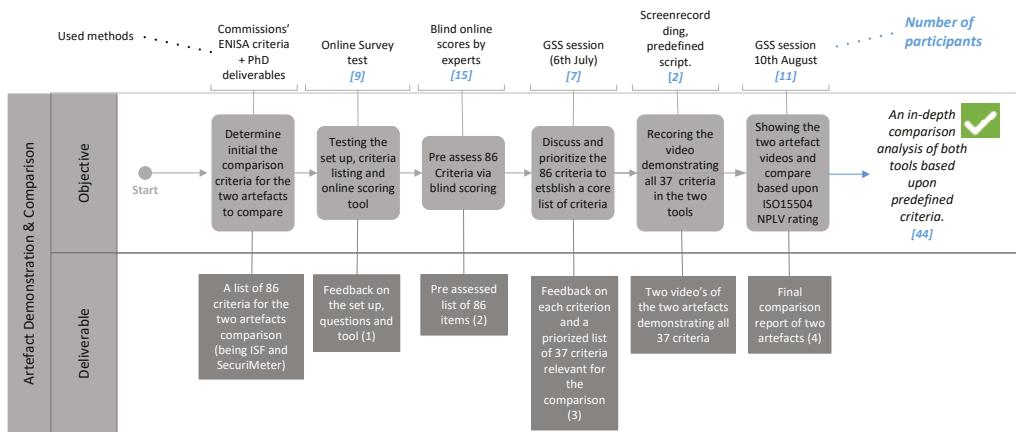


Figure 80: Artefact demonstration and comparison study research approach.

of multiple iterations to distil core comparison criteria to eventually compare two tools is visualised in the figure below. This is outlined in a comparison research approach (enclosed in the appendix) were also the role of the researcher is reduced to a minimum. By making use of this approach potential bias is reduced since the ENISA criteria list is an externally provided reference. By judging the latter, in multiple iterations, by expert panel focus groups an additional regulative cycle complements the reliability of the entire process. When making the researcher less involved in the research process and an external professional moderator (Antwerp Management School Professor) facilitates the process increases the independence and limits the influence and input merely from the researcher and increases the possibility of similar outcomes if this process was repeated. As Recker states "*independence is sometimes easier to achieve (when working with factual, objective, precise data) and sometimes harder (in interpretive research where we attempt to explain a phenomenon by interpreting available sentiments or statements about the phenomenon from participants)*" [77]. By involving multiple and different groups of people from heterogeneous professions and industries, in multiple GSS sprints increases the total population of participants and thereby yield a positive influence on the reliability. By audio recording and capturing all steps into process reports and GSS reports the entire comparison study is replicable for any other researcher.

Precision "refers to the fact that in all scientific research the concepts, constructs, and measurements should be as carefully and precisely defined as possible to allow others to use, apply, and challenge the definitions, concepts, and results in their own work" [145]. By involving multiple and different participants in multiple GSS sprints is referred to as "Relay Groups" [297]. De Vreede et al. [297] state in their paper "Athletics in Electronic Brainstorming" on differences between Relay Groups and Decathlon Groups, that by making use of multiple Relay Groups, which judge the latter of the previous group, instead of Decathlon Groups, where participants need to start from scratch, increases productivity

and group satisfaction. Both group satisfaction as well as the moderator of the GSS Session [297] increases an open atmosphere where people speak up when something is ambiguous or vague. By making use of a predefined agenda which is shared before the GSS sessions, as well as sending the participants the data upfront to prepare enables pre-questioning for clarifications or the latter to be challenged to gain precision on the latter. In addition the ISO15504 measurement scale for software capability and maturity was used to assess the predefined criteria and contributes precision.

Other academic principles Recker refer to are Credibility and Confirmability. Credibility (internal validity) refers to the fact if the researcher has substantiated his findings with sufficient evidence. Credibility in this comparison study is achieved through triangulation, maintaining a chain of evidence via; a research proposal, process reports, notes regarding decisions making throughout the process, audio and video footage and GSS Meeting reports. When implementing and maintaining a chain of evidence Confirmability (aka measurement validity) is realised. Recker states "*Confirmability suggests that qualitative research findings can be independently verified by outsiders in a position to confirm the findings (typically participants)*" for example via the appendices that encompass; the research approach, an overview of all comparison criteria, a list of participants and their characteristics, detailed process reports, meeting notes with decisions throughout the process, video presentations, GSS Meeting reports etc.

Table 21: Type of test during the comparison including dates.

TYPE OF TEST	DATE	STEP
Online survey test	20 June 2017	1a
Blind test	2 July 2017	1b
Criteria selection session	6 July 2017	1b
Video demonstration	2 Augustus 2017	2
Comparison session	10 August 2017	3

DELIVERABLES

The first an online pre-test to test the working of the meeting wizard tool was executed among 9 participants. After that step an online survey (blind, different time different place) was executed to get the initial input on all the comparison criteria. The objective is to have the participants of this session get to know the items and prepare their own session. The answers that are submitted by the participants via the online tool are captured in the GSS database and presented to the group based on the largest variance (above 40% non-consensus). The objective in this stage is to get a better understanding on the items that have a large variety. All participants that scored high are asked to provide their feedback. The feedback on all 29 discussed items is captured in the GSS Meeting tool and later on visible in the report. Below are the most relevant comments and learnings and the related decisions are highlighted.

- On the criteria “pricing” the remark was made about the fact it can be two folded; price of the product and the pricing model (e.g. user based, processor based, fixed fee, pay per use?)
- It doesn’t matter how big the company is, that’s only relevant for the scaling. Not relevant for the importance. Small companies can process large amounts of money or sensitive data.
- According to two participants a trial license is key. This is the only way, “seeing is believing”. You need to get your hands on the product. One participant scored this low in his first online submission but wants to revise his answer based on the discussion; he thinks it is really relevant.
- The view point on how to look at items is determined by the role you fulfil in the organisation. For example a manager weighs his criteria different than for example the subject matter expert (auditor).
- Initially language seems not relevant by the group but after the discussion that tools in other languages (e.g. Hebrew, Chinese) are limiting in use of acceptance. For example government in Netherlands demands tools in Dutch.
- One participant mentioned: “Some criteria are scored completely different before the session than after the group discussion within the group”
- Another participant raised: “Important is to determine the objective of the tool (doel van de tool) before selection”
- Some of the criteria are not smart was a remark of most of the participants. The ENISA list seems outdated.
- Setting the criteria and the relevance of criteria is also determined based on the level of maturity of the organisation. A less mature organisation requires more guidance.

7.4.4 COMPARISON CRITERIA

In the final round it is the objective to have the participants selects the core criteria which they think are relevant for the eventual tool comparison. With the knowledge they have gained from the previous rounds and discussions (double loop learning [148]). All criteria are presented via the Meeting Wizard iPad interface and all participants were asked to answer Yes = useful for the comparison, No = not useful for the comparison. A complete list of all comparison criteria arose, ranked based on the score of the group. Below is a list of all criteria with +85% consent, thus 6 out of 6 scored yes.

Table 22: Final list of comparison criteria derived by the expert panel on 6 July 2017.

ITEM NUMBER	TOOL COMPARISON CRITERIA DESCRIPTION (DESTILLED BY THE EXPERT BASED ON ENISA AND PHD CRITERIA) USED FOR THE VIDEO SCRIPT. REFERRED TO AS ITEM	# YES ANSWERED BY EXPERT PANEL (GSS 6TH JULY)
1	The possibility of quantifying the current and desired situations and a presentation of the steps that are necessary to bring about improvements	7
2	Dashboards on governance-, management- and operational level	7
3	List the national or international standard this tool is compliant with.	7
4	Separation of duties between user and management/maintenance	7
5	Dashboarding into Security maturity	7
6	Planning and designing multiple organisational and technical assessments at the levels of governance, management and operations,	7
7	Ability to document proof (evidence-based)	7
8	Trial before purchase, Details regarding the evaluation period of the tool (if it does exist).	7
9	Tool architecture, Specify the technologies used in this tool as well as how it is deployed (stand-alone application, web application, database used?)	7
10	Ability to identify and register relevant legislation and regulations, and the persons who are responsible and accountable.	7
11	Tool foresees different roles of users: Specify and explain if the tool supports roles of users.	7
12	Identifying the risk owners, the measures that must be taken, and the owners of these measures.	7
13	R.M. Method phases supported, Risk communication :	7
14	R.M. Method phases supported, Information processed	7
15	Specify whether the tool helps the company toward a certification according to a standard.	7
16	R.M. Method phases supported, Risk treatment :	7
17	R.M. Method processes supported: Does the tool provide Risk Management functionality? If yes, specify the processes included and how they are supported.	7
18	R.A. Method activities supported: Does the tool provide Risk assessment functionality? If yes, specify the activities included and how they are supported.	7
19	Specify available interfaces or other ways of integration with other tools	7
20	Brief description of the product, a brief description of the product containing general information, overview of functions.	7
21	R.A. Method phases supported, Risk identification :	7
22	Information Processed: Specify what kind of results/output this tool generates in each phase.	7

ITEM NUMBER	TOOL COMPARISON CRITERIA DESCRIPTION (DISTILLED BY THE EXPERT BASED ON ENISA AND PHD CRITERIA) USED FOR THE VIDEO SCRIPT. REFERRED TO AS ITEM	# YES ANSWERED BY EXPERT PANEL (GSS 6TH JULY)
23	R.M. Method phases supported, Risk assessment:	7
24	R.A. Method phases supported, Risk analysis :	7
25	Standards and norms that are present in the tool	7
26	R.A. Method phases supported, Risk evaluation :	7
27	Integration in Organization activities	6
28	Tool helps towards a certification	6
29	Specify whether it is possible to customize the tool's knowledge database to client requirements.	6
30	Flexibility of tool's database	6
31	Used in European countries: list of EU member states in which implementation is known by working group members. This includes organization as: ? European institutions (e.g. European Commission, European Union Council, European agencies). ? International organizations situated in Europe (e.g. NATO, UNO, OECD, UNESCO).	6
32	The targeted kind of users is: Operational level: guidelines for implementation planning, with a low level of detail.	6
33	The targeted kind of users is: Management level: generic guidelines.	6
34	Pricing and licensing models, Maintenance fee: the yearly fee for maintenance.	6
35	Reporting functionalities (word, csv, pdf etc)	6
36	Ability to measure the maturity on governance, management and operational levels	6
37	Trial before purchase, CD or download available :	6

VIDEOS WITH ARTEFACT DEMONSTRATIONS

Based on these criteria two video demonstrations are recorded and delivered:

- Securimeter video, accessible via: <https://youtu.be/wBNq2oyK4c4> and enclosed in the appendix. Recorded on 1 August 2017 in Ede

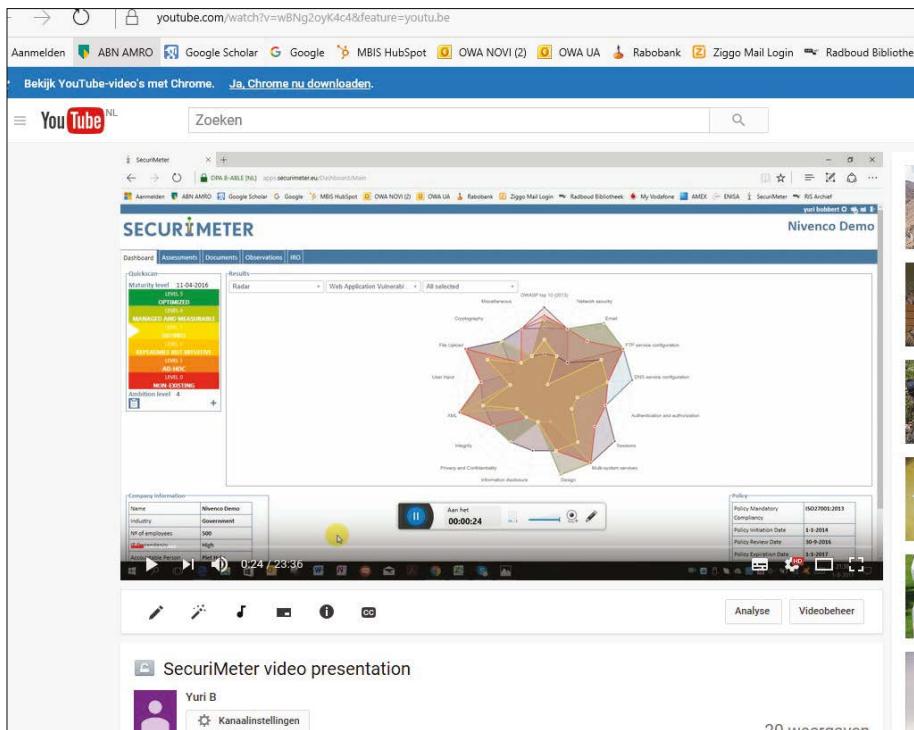


Figure 81: SecuriMeter video demonstration on YouTube used for the comparison study.

- ISF Accelerator video, accessible via: <https://youtu.be/EXLyGUFDwuQ> and enclosed in the appendix. Recorded on 18 July 2017 in Nieuwegein

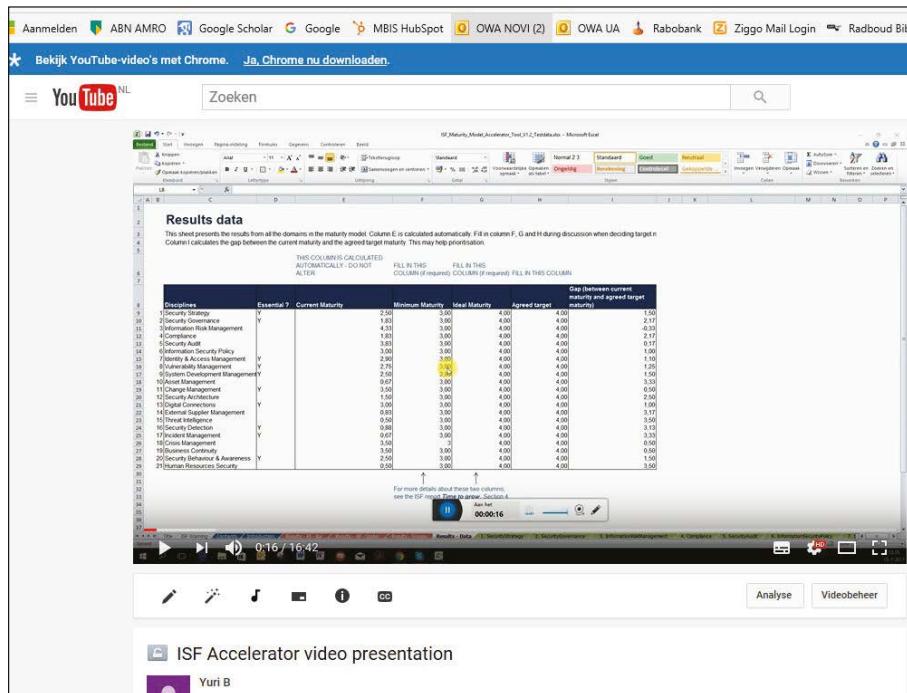


Figure 82: ISF video demonstration on YouTube used for the comparison study.

COMPARISON OF TWO ARTEFACTS

As a final deliverable the objective of the last research step 3 is to collectively compare the core functionalities of a Business Information Security (BIS) artefact.

The prepared video clips of two consultants presenting the predefined criteria in the two artefacts, being the "ISF accelerator" and the "SecuriMeter" are required to be watched by the participants prior to the GSS session. The two movies are also shown during the session and will collectively - through group discussion – be used to assess the tools on the availability of the functionalities and thereby compare the two tools.

Prior to the meeting the experts need to prepare this session by looking into the list of predefined functionalities (comparison criteria) and the video script that is used to record the presentations. By looking into this list prior to watching the video the experts will be better prepared for the group session. The session is moderated by Professor Hans Mulder of Antwerp University. The entire list of all 37 criteria items including the video demonstrations

of the two artefacts were shared one week prior to the session. In the table below the scores of both tools are presented. The variance represents the deviation of the scores of the experts. The deviations above 40% are discussed in the group and further detailed in the next analysis chapter.

Table 23: Expert scores on SecuriMeter matching the criteria ranked on rating.

CRITERIA ITEM	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
35	Reporting functionalities (word, csv, pdf etc)		
	4	1	0%
12	Identifying the risk owners, the measures that must be taken, and the owners of these measures.		
	3,9	1	20%
29	Specify whether it is possible to customize the tool's knowledge database to client requirements.		
	3,9	3	22%
25	Standards and norms that are present in the tool		
	3,8	1	27%
7	Ability to document proof (evidence-based)		
	3,8	0	26%
37	Trial before purchase, CD or download available		
	3,8	3	44%
4	Separation of duties between user and management/maintenance		
	3,8	1	27%
3	List the national or international standard this tool is compliant with.		
	3,8	1	40%
5	Dashboarding into Security maturity		
	3,7	1	31%
8	Trial before purchase, Details regarding the evaluation period of the tool (if it does exist).		
	3,7	2	44%
36	Ability to measure the maturity on governance, management and operational levels		
	3,7	1	43%
16	R.M. Method phases supported, Risk treatment		
	3,6	1	44%
11	Tool foresees different roles of users: Specify and explain if the tool supports roles of users.		
	3,6	2	46%

CRITERIA ITEM	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
20	Brief description of the product, a brief description of the product containing general information, overview of functions.		
	3,6	1	61%
2	Dashboards on governance-, management- and operational level		
	3,5	0	52%
1	The possibility of quantifying the current and desired situations and a presentation of the steps that are necessary to bring about improvements		
	3,5	0	59%
28	Tool helps towards a certification		
	3,5	3	47%
14	R.M. Method phases supported, Information processed		
	3,5	3	67%
26	R.A. Method phases supported, Risk evaluation		
	3,4	1	33%
13	R.M. Method phases supported, Risk communication		
	3,4	2	46%
15	Specify whether the tool helps the company toward a certification according to a standard.		
	3,4	2	46%
17	R.M. Method processes supported: Does the tool provide Risk Management functionality? If yes, specify the processes included and how they are supported.		
	3,4	1	53%
6	Planning and designing multiple organisational and technical assessments at the levels of governance, management and operations		
	3,4	0	59%
9	Tool architecture, Specify the technologies used in this tool as well as how it is deployed (standalone application, web application, database used?)		
	3,4	3	57%
33	The targeted kind of users is: Management level: generic guidelines.		
	3,3	2	44%
22	Information Processed: Specify what kind of results/output this tool generates in each phase.		
	3,3	1	43%

CRITERIA ITEM	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
19	Specify available interfaces or other ways of integration with other tools 3,1	3	62%
10	Ability to identify and register relevant legislation and regulations, and the persons who are responsible and accountable. 3,1	1	70%
21	R.A. Method phases supported, Risk identification 3,1	1	55%
32	The targeted kind of users is: Operational level: guidelines for implementation planning, with a low level of detail. 3	1	42%
30	Flexibility of tool's database 3	2	54%
24	R.A. Method phases supported, Risk analysis 2,9	2	73%
23	R.M. Method phases supported, Risk assessment 2,9	2	73%
18	R.A. Method activities supported: Does the tool provide Risk assessment functionality? If yes, specify the activities included and how they are supported. 2,9	2	49%
27	Intergration in Organization activities 2,4	6	53%
34	Pricing and licensing models, Maintenance fee: the yearly fee for maintenance. 2,2	6	98%
31	Used in European countries: list of EU member states in which implementation is known by working group members. This includes organization as: European institutions (e.g. European Commission, European Union Council, European agencies). International organizations situated in Europe (e.g. NATO, UNO, OECD, UNESCO). 2,2	5	90%

Table 24: Expert panel scores on ISF Accelerator matching the criteria ranked on rating.

CRITERIA ITEM #	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
34	Pricing and licensing models, Maintenance fee: the yearly fee for maintenance. 3,6	6	53%
20	Brief description of the product, a brief description of the product containing general information, overview of functions. 3,5	5	33%
5	Dashboarding into Security maturity 3,5	1	54%
9	Tool architecture, Specify the technologies used in this tool as well as how it is deployed (standalone application, web application, database used?) 3,4	4	70%
35	Reporting functionalities (word, csv, pdf etc) 3,3	1	67%
1	The possibility of quantifying the current and desired situations and a presentation of the steps that are necessary to bring about improvements 2,8	1	50%
33	The targeted kind of users is: Management level: generic guidelines. 2,8	1	40%
36	Ability to measure the maturity on governance, management and operational levels 2,7	1	52%
2	Dashboards on governance-, management- and operational level 2,6	0	51%
22	Information Processed: Specify what kind of results/output this tool generates in each phase. 2,6	2	71%
29	Specify whether it is possible to customize the tool's knowledge database to client requirements. 2,5	1	75%
27	Intergration in Organization activities 2,3	7	29%
25	Standards and norms that are present in the tool 2	2	63%

CRITERIA ITEM #	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
31	Used in European countries: list of EU member states in which implementation is known by working group members. This includes organization as: ? European institutions (e.g. European Commission, European Union Council, European agencies). International organizations situated in Europe (e.g. NATO, UNO, OECD, UNESCO).		
	1,6	6	80%
7	Ability to document proof (evidence-based)		
	1,6	2	46%
19	Specify available interfaces or other ways of integration with other tools		
	1,5	1	68%
3	List the national or international standard this tool is compliant with.		
	1,4	3	66%
30	Flexibility of tool's database		
	1,4	3	66%
15	Specify whether the tool helps the company toward a certification according to a standard.		
	1,4	2	46%
8	Trial before purchase, Details regarding the evaluation period of the tool (if it does exist).		
	1,3	7	29%
10	Ability to identify and register relevant legislation and regulations, and the persons who are responsible and accountable.		
	1,3	2	63%
28	Tool helps towards a certification		
	1,3	4	30%
23	R.M. Method phases supported, Risk assessment		
	1,2	1	40%
24	R.A. Method phases supported, Risk analysis		
	1,1	1	20%
32	The targeted kind of users is: Operational level: guidelines for implementation planning, with a low level of detail.		
	1	3	0%
6	Planning and designing multiple organisational and technical assessments at the levels of governance, management and operations		
	1	1	0%
37	Trial before purchase, CD or download available		
	1	1	6%

CRITERIA ITEM #	CRITERIA ITEM DESCRIPTION RATING	ABSTAIN	VARIABILITY
4	Separation of duties between user and management/maintenance		
	1	0	0%
12	Identifying the risk owners, the measures that must be taken, and the owners of these measures.		
	1	2	0%
21	R.A. Method phases supported, Risk identification		
	1	1	0%
16	R.M. Method phases supported, Risk treatment		
	1	1	0%
18	R.A. Method activities supported: Does the tool provide Risk assessment functionality? If yes, specify the activities included and how they are supported.		
	1	1	0%
14	R.M. Method phases supported, Information processed		
	1	1	0%
13	R.M. Method phases supported, Risk communication		
	1	2	0%
17	R.M. Method processes supported: Does the tool provide Risk Management functionality? If yes, specify the processes included and how they are supported.		
	1	1	0%
26	R.A. Method phases supported, Risk evaluation		
	1	1	0%
11	Tool foresees different roles of users: Specify and explain if the tool supports roles of users.		
	1	2	0%

The entire GSS meeting Wizard report can be found in the appendix, including the process report of the meeting. This can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

DATA ANALYSIS SECURIMETER

When doing the analysis on the scores from the experts judgment we round up the figures to one single digit. For example; 2.4 being 2, and 2.6 being 3.

34 items of the predefined criteria items scored 3 (largely achieved) and 4 (fully achieved). This means 91,9% of all 37 criteria are "largely" or "fully present" in the SecuriMeter. The entire list of all criteria including the scores and variance between the participants is listed below.

From all comments made by the participants submitted in the system during the session I analysed them all and I will address the relevant remarks from the participants that require additional explanation or reflection.

ITEM 20. BRIEF DESCRIPTION OF THE TOOL.

-One of the participants raised; brief description is not a comparison criteria. It cannot be found in the tool.

ITEM 30. FLEXIBILITY OF TOOLS DATABASE

-A comment was made that "never sharing customer data" was mentioned in the question. It was actually in the answer given (not in the question) by the presenter of the tool to make explicit how SecuriMeter deals with confidential data in the database and the fact that it (customer data) is not shared.

ITEM 27. INTEGRATION IN ORGANISATION ACTIVITIES.

Hard to present for both tools since this requires more time to make this explicit and the videos were limited in time. Comparing this criteria also depends on which functionality of the tool you want to present for this since most of the functionalities can integrate into numerous processes, e.g. risk management processes, reporting processes, testing processes etc.

ITEM 11. TOOL FORESEES DIFFERENT ROLES OF USERS: SPECIFY AND EXPLAIN IF THE TOOL SUPPORTS ROLES OF USERS.

This is a relevant comment since securely separate users for example via Multi Factor Authentication (MFA) is not presented and present in both tools. This could well be a future requirement.

ITEM 15. SPECIFY WHETHER THE TOOL HELPS THE COMPANY TOWARD A CERTIFICATION ACCORDING TO A STANDARD.

Both presentations did not specifically present how this could be achieved. This requires additional information/demonstration via for example a product walkthrough.

Item 3: List the national or international standard this tool is compliant with.

Good remark from one of the participants that the tool does the listing (is the engine), it is not about having all the standards. But to support working with all the standards that were listed prior to implementation of the tool.

DATA ANALYSIS ISF ACCELERATOR

When analysing the results of the ISF tool scores based on the same digit roundup method we observe 11 items of the predefined criteria items scoring 4 (fully achieved) and 3 (largely achieved) based on the ISO15504 NPLV scoring. This means that 29,7% of the criteria are fully or largely present in the ISF Accelerator tool. If we take into consideration the

remark that the participants raised at item number 20; a brief description of the product is not a criteria rather than something that is handy to have so you immediately know the core capabilities of the tool. It is not "in the tool" as one of the experts mentioned. This criteria scored 3.5 in the ISF scoring. One could argue if this criterion should not have been withdrawn in the initial selections.

Additional analysis was done on the 4 comments the experts made during the scoring.

34. Pricing and licensing models, Maintenance fee: the yearly fee for maintenance.

ISF tooling is part of a larger whole. Namely, a community body with extensive materials such as tools.

27. Integration in Organization activities

As most Microsoft Excel users know spreadsheets offer multiple ways to interface or automate things (e.g. via macro's, scripts etc.). This was not explicitly mentioned during the presentation.

7.5 ADDITIONAL INSIGHTS AFTER DEMONSTRATING, EVALUATING AND COMPARING THE ARTEFACT

In 2000 de Vreede et al. [297] stated that discussion groups working on outcomes of others have better results than groups that start from scratch. De Vreede et al. refer to Decathlon Groups when Groups need to start from scratch and Relay Groups when they work on previous collected data. De Vreede stated: "*Relay groups appeared to be more productive than Decathlon groups, in particular in terms of elaborations to previous contributions*" *Relay groups also produced slightly more unique ideas, but not significantly. Hence, we may conclude that overall a Relay method is preferable in terms of productivity than a Decathlon method.* In this research project the last expert group used the data of the previous group in order to enable productivity of the group, since rating such an amount of criteria and compare the tools based on these criteria may take multiple hours and may be a mental stretch. This might have an impact on the participant's satisfaction. As De Vreede et al. continue in their research "*Relay groups were also found to be more satisfied*", in terms of interest accommodation.

With this knowledge an additional step was added to the GSS meeting. In addition to the comparison of the two artefacts the experts were also asked, based on their prior gained and shared knowledge, to brainstorm on the research question "*Which parameters that influence the Maturing Business Information Security (MBIS) process can be considered as requirements for an artefact designed to capture, measure and report the MBIS process?*" The objective of this question was to gain a qualified insight through discussion and listing of parameters via experts' opinions. This seems specifically interesting for me as a researcher

to see if the experts perceive the same artefact requirements compared to the ones I have gained via this research project. From all 98 answers given by the experts I will highlight the most relevant one that are "already part of the SecuriMeter" artefact, marked as AP, "not yet in the artefact" marked as NP, or are a "part of the analysis method", marked as PAM. PAM refers to the analysis method which enables knowledge sharing, consensus building on priorities, decision-making, stakeholder engagement, increasing the awareness and enables reflection. PAM encompasses two artefacts:

One being the collaborative analysis method that enables team collaboration to define the parameters for analysis of the BIS maturity and two the SecuriMeter tool that supports the administrative work (for measuring and reporting purposes), which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational). A subset of the list that was derived via experts is displayed in the table below. The relevant -new - items that gave new / or inspiring insights on the topic, are listed including my reflection (as a researcher).

Interesting finding from the expert participants is that most of the submitted answers relate to either "preconditions" or "enablers" of the BIS improvement process such as; tone at the top, culture, enable lower in the organisation decision-making, knowledge, education etcetera. These items are most of the time collectively determined based on strategic objectives, regulatory requirements or the type of industry an organisation is in. Therefor the majority, 55 of the total 98, of the items were marked as "part of the analysis method". This means that the majority of the parameters raised by the experts are subject to some form of -team- collaboration.

21 items of the total 98 are already functionalities present within the SecuriMeter artefact.

10 items are both subject to PAM as well as a future requirement since these are not present in SecuriMeter yet. These items are interesting and reflected below since they can serve as future artefact requirements. 18 items are not yet present but can well be considered as a requirement and are potential backlog items that the developers can take into consideration for the next sprints. Therefor this additional comparison was a meaningful exercise.

Table 25: Abstract of the 98 requirement suggested by the experts on multiple levels.

ORGAN-ISA-TIONAL LEVEL	ARTEFACT REQUIRE-MENT SUGGESTION SUBMITTED BY THE EXPERTS	AP = AL-READY PRESENT IN SECURIME-TER	NP = NOT PRESENT IN SECURIME-TER	PAM = PART OF THE ANALYSIS METHOD	RESEARCHERS REFLECTION ON SUGGESTIONS
GOVERNANCE					
G	Needed: governance structure in which interconnectivity exists between stakeholder on several layers			PAM	collectively fill in the questionnaires via GSS
G	Link to business objectives			PAM	Can be done via referencing the domains of a standard towards a strategic objective
G	country of operation		NP		Very relevant functionality for a multi-national dealing with multiple foreign regulatory requirements
G	Awareness of what the desired level of maturity is: compliance-driven or self-imposed goals?	AP		PAM	Defining the desired level can be done in SecuriMeter, and how the organisation is engineered in its processes (control oriented, self-imposed, or threat oriented) can also be defined. Stating this is always subject to debate on interpretation for example via GSS.
MANAGEMENT					
M	freedom for taking action			PAM	Needs to be set and mandated by management, for example by working in small Agile teams (DevOps way of working).
M	Support prioritizing specific risks and measures: best value for your money.	AP		PAM	This is partly present but can be improved via the IRO. Making the IRO part of a collaborative process to prioritize risk treatments tuned to the value for money
M	Translate known risks into costs of business discontinuity or lost opportunity		NP	PAM	This is partly present but can be improved via the IRO. Making the IRO part of a collaborative process to link risks to lost opportunities

ORGANISATIONAL LEVEL	ARTEFACT REQUIREMENT SUGGESTION SUBMITTED BY THE EXPERTS	AP = ALREADY PRESENT IN SECURIMETER	NP = NOT PRESENT IN SECURIMETER	PAM = PART OF THE ANALYSIS METHOD	RESEARCHERS REFLECTION ON SUGGESTIONS
M	security as part of KPIs, yearplan of employees		NP	PAM	Integrate with HR rewarding mechanisms
M	tone at the bottom			PAM	
M	available budget		NP		
M	look outside the organisation and learn from others their mistakes		NP		
M	Trustworthyness or (un)certainty of data. Data regarding the maturity of a control deteriorates over time.		NP		
M	Different mitigation options incl pro's and con's		NP	PAM	
M	reliability of management information		NP		Reliability can be improved via sign off process and retention policies on the information submitted in SecuriMeter
M	management approach/type		NP	PAM	Increasingly important due to agile way of working were decision making is delegated more down in the organisation and teams.
M	level of knowledge and expertise of management		NP	PAM	Current knowledge and expertise of management can be assessed via SecuriMeter (e.g. via number of certifications or taken courses), defining the gap can also be done by setting clear knowledge requirements per maturity level per domain. Improvement is needed in explicating the expertise gap
OPERATIONS					
O	every 4 years : review all operations for usefulness and lean		NP		

0	all security operations must have a purpose . if not, DELETE		NP		Enforce alignment of controls towards business objectives. Mandatory functionality to reference a control towards an objective
0	Security data must be an integral part of operational data		NP	PAM	Therefor requires the same BIA process as regular data.
0	make improvements visible to employees	AP		PAM	
0	Include operations as active component in improvement of security, not just as only serving for execution of what is decided at other levels		NP	PAM	
0	skilled employee		NP	PAM	Current skills level can be assessed via SecuriMeter (e.g. via number of certifications or taken -online-courses), defining the gap can also be done by setting clear knowledge requirements per maturity level per domain. Improvement is needed in explicating the expertise gap

7.6 CONCLUSIONS TO THE ARTEFACT DEMONSTRATION AND EVALUATION

The proposed method described in this thesis needs to enable a collective analysis through team collaboration and deliver an administrative tool that facilitates the process of capturing, measuring, storing and reporting the required BIS data in order to improve the Maturity of Business Information Security. According to the comparison study held among experts this "administrative tool" delivers the majority of the predefined criteria. Although there was much debate on the accuracy of the provided ENISA list (2006), as well as the comparability. One participant comments; "*Comparing a tool based on Excel and a SaaS tool is comparing apples and oranges*". Despite the debate this comparison actually validated the delivery of the artefact and its requirements via a rigours process. The final result is a validated tool that supports the administrative work (for measuring and reporting purposes), which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational) to boards, owners and other stakeholders. The ability of addressing multiple layers such as Governance, Management and Operations was acknowledged by the entire expert panel via item 4, 5, 12 and report accordingly towards stakeholders, proven via item 3, 5, 6, 7, 9, 10 presented in Table 26

Table 26: List of artefact requirements that are present in the SecuriMeter.

	Criteria derived from the deliverables in the PhD research:	Nr of experts agree (total 7)	Relevance for comparison according to the expert panel of 6th July 2017 (in percentages)	Present in SecuriMeter artefact according to the 11 experts (on ISO15504 NPLF Scoring) of 0th August 2017	
1	Ability to identify and register relevant legislation and regulations, and the persons who are responsible and accountable.	7	100%	3	Largely Achieved
2	Identifying the risk owners, the measures that must be taken, and the owners of these measures.	7	100%	4	Fully Achieved
3	Ability to document proof (evidence-based)	7	100%	4	Fully Achieved
4	Planning and designing multiple organisational and technical assessments at the levels of governance, management and operations,	7	100%	3	Largely Achieved
5	Dashboards on governance-, management- and operational level	7	100%	4	Fully Achieved

	Criteria derived from the deliverables in the PhD research:	Nr of experts agree (total 7)	Relevance for comparison according to the expert panel of 6th July 2017 (in percentages)	Present in SecuriMeter artefact according to the 11 experts (on ISO15504 NPLF Scoring) of 0th August 2017	
6	The possibility of quantifying the current and desired situations and a presentation of the steps that are necessary to bring about improvements	7	100%	4	Fully Achieved
7	Various benchmarking capabilities, specific to the sector concerned,*	5	71%	NA	NA
8	Separation of duties between user and management/maintenance	7	100%	4	Fully Achieved
9	Reporting functionalities (word, csv, pdf etc)	6	86%	4	Fully Achieved
10	Dashboarding into Security maturity	7	100%	4	Fully Achieved
11	Standards and norms that are present in the tool	7	100%	4	Fully Achieved
12	Ability to measure the maturity on governance, management and operational levels	6	86%	4	Fully Achieved
13	API (to extract data from various sources)*	4	57%	NA	NA

* these items are not measured since they had little consensus (<86%) by the expert panel

This panel of eleven experts in the field validated the working of the artefact. According to this expert panel ten out of the thirteen artefact requirements that are described in this thesis are relevant for a BIS tool (artefact). All experts agreed that all requirements are fully or largely available in the established artefact.

CONCLUSIONS AND FUTURE RECOMMENDATIONS

In conclusion we can state that according to the guidelines for artefact demonstration and evaluation provided by Johannesson and Perjons [73] we summarise the problem, the treatment of the problem via requirement setting, the method used to evaluate the artefact and the level of stakeholder engagement. In the table below we summarise the most important evaluation methods and in the figure is displayed how these methods relate to the Framework [73].

Table 27: Summary of the evaluation methods used.

Case	Requirement	Evaluation method
Key BIS management information	Dashboard on policy status, risks and evidence	POC and stakeholder interviews
Key BIS governance practices and KSF	Assessment questionnaire	Real-life and stakeholder participation during assessments and sessions (with boards ¹⁾)
Key BIS management interventions	BIS maturity Assessment questionnaire	POC and stakeholder interviews (mid-market organisations). Also real-life application of +100 maturity assessments between 2011-2015)
Insight into BIS metrics	List of predefined metrics	Via the evaluation register (see the Appendix) that is filled by stakeholder feedback
Use of existing management models	Knowledge items / Scope and context items / Stakeholder analysis	GSS research session at Erasmus University with 28 participants that represent stakeholders

An important conclusion and future recommendation is proposed by Ge and Helfert [299]. The authors proposed a framework for guiding "*experimental evaluation in design science, consisting of three components: artefact, experiment, and data analysis*". This enables a more iterative and creative process of development, with the limitation that the artefact is overloaded with irrelevant requirements. Tremblay [147] et al. "*investigate the use of focus groups for artefact evaluation, making a distinction between exploratory focus groups that study an artefact in order to suggest improvements for further design (formative evaluation)*". This is similar to what was done in this research project in case 1 with the use of GSS for identifying key BIS management information. And the other method is a confirmatory focus group. That aims to establish the utility of an artefact in field use (summative evaluation), similar to what was done via the last two artefact evaluations in this research project. The scoping was very tight on summative evaluation and it set the direction for business development (i.e. valorisation).

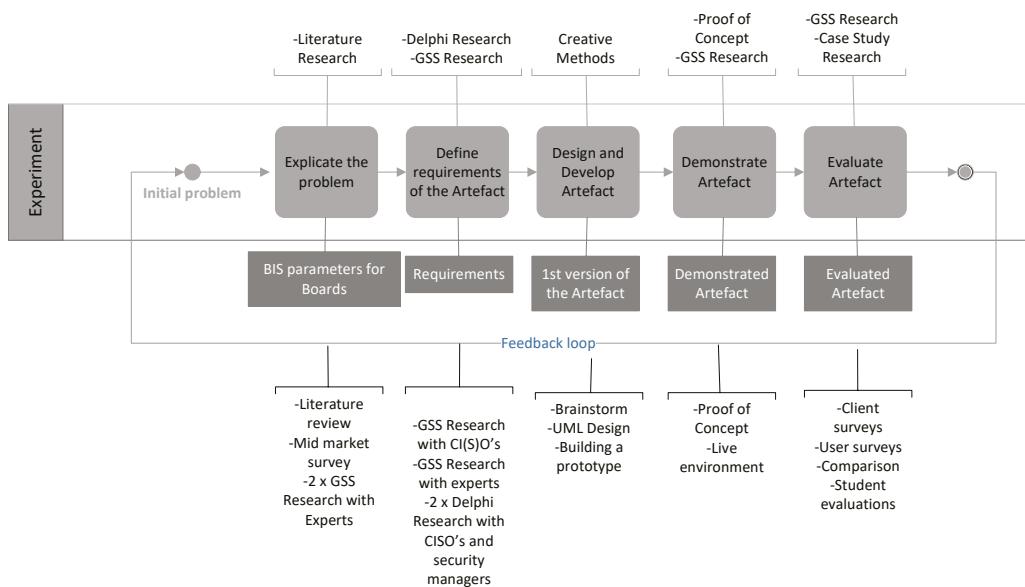


Figure 83: Methods to demonstrate and evaluate the artefact based on Johannesson and Perjons [73]

8

FINDINGS, CONCLUSIONS, LIMITATIONS AND CONTRIBUTIONS

This chapter contains the overall findings, conclusions and limitations of this research project. It reveals the practical and academic contribution and how the process of valorisation is realised due to rigorous exploration and practical exploitation of the artefact.

8.1 RESEARCH FINDINGS

This research project delivers a conceptual framework for BIS with parameters that influence the BIS maturity at management as well as governance level (Board of Directors) as well as insights into factors that influence the BIS maturity such as barriers.

In chapter 2 a multi-method research approach is proposed and used throughout this project. This method, based upon GSS, utilises knowledge sharing, consensus building on priorities, make decisions, enable stakeholder engagement, e.g. through collaboration it contributes to the increase of awareness and enables reflection. This enables to break silo's and reflect on learnings in order to improve.

The delivered design artefact-tool supports the analytical and administrative work, of measuring and reporting, which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational). It thereby removes the current troubles of evidencing-documents that are currently scattered all over the company. The delivered artefact creates one single source of truth. The complete method is coined MBIS method and is visualised in Figure 84: The MBIS method and PDCA-based activities.

More than 40 highly qualified, board-level professionals contributed to the artefact requirements study. The outcome revealed that the current BIS measurement monitoring and reporting tooling is lacking **79%** in the necessary requirements to do proper security administration. In comparison of a financial accounting system this would imply a major compliance default that could lead to bankruptcy.

According to the expert panel **91%** of the required functionalities are present in the artefact that is established in this research project.

ANSWERS TO THE RESEARCH QUESTIONS

The main research question set forward in chapter 1 in this thesis "*How can we establish method, which utilises best practices and collaboration for improving BIS maturity?*" is answered in multiple ways. Chapter 2 presents the method that was developed, to strengthen the collaboration and decision-making processes needed in order to address and solve BIS-related problems. GSS was applied as a research technique to determine the requirements among stakeholders and to prepare or guide the stakeholder-user group when discussing the implementation (making the tool fit for purpose). The administrative tool used to support this PDCA-based approach and to capture, measure and report it is called the 'SecuriMeter' artefact, which is presented through this research. The utilisation of best

practices such as ISO, using a DSR methodology that is based on the work of numerous DSR research scientists such as Winter, [300], Dietz and Hoogervorst [301], Albani et al. [302], Van Aken et al. [225], Wieringa [146], Hevner et al. [138], Johannesson and Perjons [73] and is collectively referred to as the 'MBIS method' as visualised in Figure 84. Throughout the research project multiple participants mentioned that determining the current and desired state is subject to collaboration with multiple stakeholders. One of the participants mentioned "*Collective submitting the answers in the tool with the different roles/ responsibilities in the organisation raises awareness and defines individual responsibilities in a collective approach to reach a mature organisation*". An important finding is that the proposed MBIS method enables a collective analysis through team (BoD, MT) collaboration and process the required data in the administrative tool to measure, monitor and report. Chapters 4 and 5 elaborate how the numerous qualitative research methods, proposed in Chapter 2, such as GSS research and Delphi contribute to a qualitative view into enablers and disablers of MBIS and how GSS and Delphi utilise the establishment of parameters that can be considered by board of directors or executive management. Chapter 4 produces a qualitative view from the perspective of experts. The extra empirical validation on the research data was performed on the target group and revealed interesting findings on the four main barriers that limit the MBIS process. The target group raised the following issues: management and organisation, perception and attitudes, knowledge and skills and budgets as the main barriers to the MBIS process. These items were reframed in the conceptual model that was used for further investigation of MBIS parameters and helped define the research assumptions according to Whetten [150]. The reframing is as follows:

BARRIERS	PARAMETERS OF INFLUENCE
Management and organisation	Management and organisation (1)
Perception and attitudes	Part of the Culture (3)
Knowledge and skills	Part of the Resource capabilities (2) of the organisation and the people
Budget	Not perceived as a direct barrier and not raised as an intervention for example "more money". We assume therefore that budget is not seen as a barrier (only 12%) but as a dependent variable that can and will be influenced by all of the above

Chapter 4 also propose the seven preconditions organisations need to consider before attending the MBIS process. These are qualitative preconditions that were raised by experts and target groups of CISO's CIO's IT managers and security managers. The collective or individual application of the preconditions varies in influence on the effect of the individual intervention [218]. Along with these preconditions this research resulted in a qualified list of core interventions that are prioritised by mid-market organisations. These core interventions are established (source is ISO) due to expert panel assessment and prioritisation via GSS, based on "ease of implementation" and "effectiveness". The proposed long list of ISO27002

controls, e.g. interventions answers research question two and the final list of derived interventions answers question five. This chapter 4 demonstrates the use of best practices from the existing communities to examine the potential artefact requirements. These are later on validated via survey research by 40 organisations representing the target group, mid-market organisations. Due the variety of the participating organisations it is fair to state that this core set is generalizable and valid for mid-market organisations. By this research, research questions 1 to 6 were answered and new insights for the next research phase were gathered. Research questions one to six were:

1. What is BIS maturity, based on the definitions derived from best practices and literature?

Answer: Out of chapter 2 we have derived BIS Maturity as a state, process or period of being mature as an organisation when it comes to Business Information Security, expressed via a maturity model which constitutes of multiple levels with predefined criteria. With Business Information Security we address the entire End-to-End process of information processing including all relevant stakeholders.

2. Which best-practice interventions are currently used to improve BIS maturity?

Answer: In chapter 3 and 4 multiple Information Security frameworks and maturity models are described. The selected long list of ISO27002 controls, e.g. interventions is used by the majority of the organisations and therefor used in this research to examine core interventions that can be promoted to artefact requirements in the next sections of the research.

3. Which barriers do organisations experience when applying BIS interventions?

Answer: In section 4.4.7 of chapter 4 a list of Main barriers for MBIS according to the experts is derived and categorised.

Main barriers for MBIS according to the experts

4. Which barriers have been identified in mid-market organisations?

Answer Table 6: Top intervention suggestions according to mid-market organisations. display the main barriers derived from the research. Being Management and organisation, Perception and attitudes, Knowledge and skills, Budget

5. Which of the identified BIS interventions are practical in such organisations?

Answer: In Table 6 the top BIS intervention that are practical according to mid-market organisations is proposed.

6. What are the general organisational preconditions for the application of the core set of BIS interventions?

Answer: The organisational preconditions for the application of the core set of BIS interventions that were derived in section 4.7 of chapter 4 are:

- Identify applicable (mid-market) laws and legislation.
- Perform risk and impact analysis in order to justify the implementation of necessary interventions in order to achieve the desired security maturity level.
- Apply relevant norms in order to comply with law, legislation or regulations or a framework that is derived from these norms, for example COBIT.
- Involve management about the business impact of not having these essential interventions in place.
- Increase the awareness of security throughout the organisations since human error is a predominately cause. Train and educate with focus on the correct perception about security on the technical as well as the business side of the organisation.
- Measure and monitor all potential technical and organisational vulnerabilities (security assessments) as a continuous process in order to be in control and achieve the desired level of security maturity.
- Continuous maintain knowledge and skills that are essential to keep being "in control".

An important finding that was gained from the MBIS research journey described in Chapter 4 was the emphasis most of the respondents gave to the fact that the engagement of senior management and board is essential for the successful attending the process of improving BIS. This organisational level can provide strategic direction into factors such as clear stakeholder expectations, regulations, business goals and risk appetite. All of these factors are of influence but were most of the time absent by the examined companies in Chapter 4. This was demonstrated by the 39% that scored 2 out of 5 and 21% scored 1 out of 5 on the COBIT maturity ladder.

Therefore the research in Chapter 5 was conducted with the objective to provide answer to research question:

7. What is a useful framework for Business Information Security Governance practices, according to the academic literature on the subject and the views of experts?

Answer: With the objective to develop a core set of practices that contemporary boards can use to direct, monitor and control Business Information Security, chapter 5 led to Governance practices suitable for Business Information Security, distilled by expert panel research. Table 9 proposes the top 10 of these Business Information Security Governance practices being; 1. Determine Roles, 2. Corporate internal communication, 3. Awareness at level of Boards of Directors, 4. Board and Senior Management Leadership, 5. Lessons learned, 6. Transparency, 7. Determine risk appetite, 8. Internal control, 9. Regular

reporting, 10. Ensuring the integrity of the corporation.

A prioritised set of practices and critical success factors was derived from 228 practices out of +100 literature sources varying from academia to practitioner-oriented. The direct result is a list of 22 practices that can function as a framework of BISG practices, e.g. parameters of controls for boards. Main conclusion from this research is that these governance practices need to be taken into account before an organisation starts any BIS improvement initiative. Ontological and epistemological challenges can be mastered by collaborative exchanging viewpoints, meanings and opinions on the topic, based on these 22 items, that traditional ad-hoc and project based approaches absence. The qualitative research conducted in Chapter 5, due to applying a collaborative analysis method such as GSS, also revealed the positive effect that GSS has via group interaction and group thinking, such as management teams and boards. Besides having a facilitating function, it also suits the objectives of generating, capturing and sharing the necessary knowledge in order to overcome the epistemological challenges of knowledge management, e.g. scoping knowledge raised in chapter 2. The research in Chapter 5 indirectly answers the main research question by showing that GSS provides a collaborative method that utilises best practices, the best practices in this research being the governance practices from the literature.

The research projects described in chapters 4 and 5 about management and governance practices delivered a conceptual framework for BIS-related Design Science Research methodologies as proposed in chapter 2. It derived two sets of design requirements to establish into the artefact. Chapter 6 and 7 elaborate on five cases of practical business problems that were addressed by applying the DSR methods in designing the artefact requirements to be presented in Chapter 7. Important findings from chapter 6 are the additional insights into metrics Boards can measure and report on, the successful use of management models to address strategic forces and CI(S)O's can use to bring their message across and the essence of creating a transparent and open culture (whistle blowing) in order to continuously learn. Main conclusion of chapter 6 is the value-add of the proposed DSR method to explicate problems and the impact for stakeholders.

The requirements set forward in chapter 6 and presented in chapter 7 are not limited. Numerous other requirements are described in Chapter 7 and validated by experts. These requirements were set together in collaboration with a network of eco partners. An evaluation of the artefact requirements was made in Chapter 7 and is still being done as part of the continuous development process visualised in the PDCA (see Figure 84). Main conclusion from chapter 7 is that BIS improvement is not only about administrative tooling, but about collaborating, and mutually setting objectives and determine priorities. The proposed method foresees in the collaboration as well as the administration that is required during the maturing process.

8. Which parameters that influence the Maturing Business Information Security (MBIS) process can be considered as requirements for an artefact designed to capture, measure and report the MBIS process?

Answer: This can be answered by the enumeration of the five cases of business problems that were translated into requirements in the artefact and can be considered as parameters to capture, measure and control the MBIS process;

CASE	PROBLEM	ARTEFACT REQUIREMENT	FORM
1.Key BIS management information	The absence of a centralised fact-based view on BIS (dashboard)	Dashboard on policy status, risks and evidence	Dashboard
2.Key BIS Governance practices and KSF	The absence of Governance practices and Critical Success Factors for Business Information Security	Assessment questionnaire	Functional
3.Key BIS management interventions	The absence of a core set of interventions that can be applied to enhance the maturity level of BIS	BIS maturity Assessment questionnaire	Functional
4.Insight into BIS metrics	Absence of effective metrics for Governance, management and operational level in order to measure the MBIS process	List of predefined metrics	Non-functional & functional
5.Use of existing management models	Absence of knowledge items into strategic external forces of influence that is relevant in the BIS strategy formulation	Knowledge items / Scope and context items / Stakeholder analysis	Functional & Environmental

For the articulation and validation of the requirements of the artefact, the GSS helped in shifting the interventions based on the average and variance of the group. And prioritise based on practical appliance of a total score on effectivity of the intervention of > 1.5 and variance of the group. GSS made it possible to assemble 22 BISG practices based on numerous criteria and delete low scoring items and discuss the high variances among experts.

Research question nine can be answered through the research conducted in Chapters 6 and 7;

9. How do these artefact requirements contribute to solving the business problems and meeting stakeholders' needs?

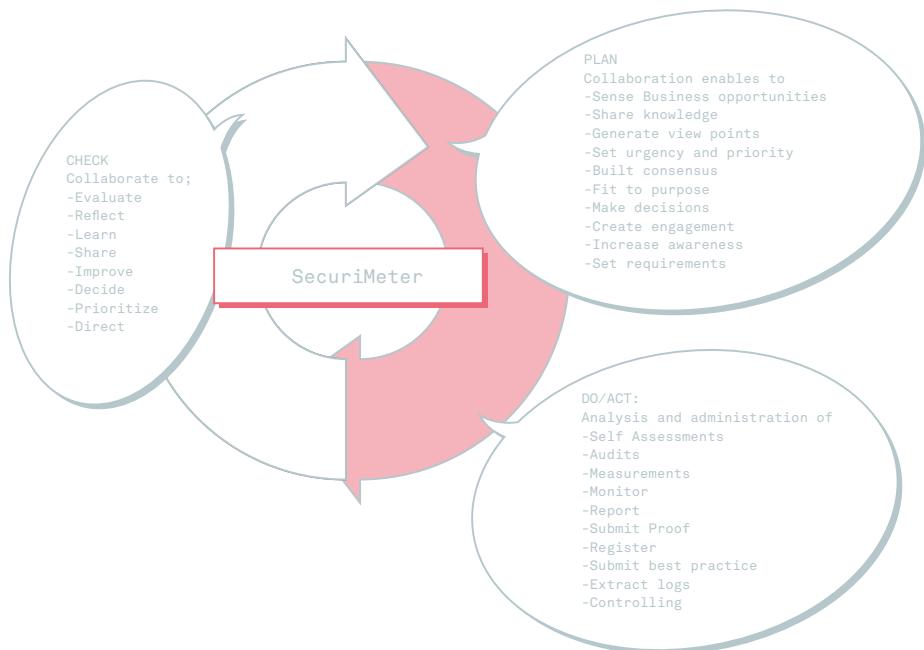


Figure 84: The MBIS method and PDCA-based activities.

Answer: The contribution of the artefact is that organisations and their stakeholders can increase the security maturity by applying the artefact and the predefined assessments, standards, reports etc. By periodically executing for example the predefined assessments all relevant items (people, process, technology) are addressed, monitored, proofed and reported continuously. Capturing and providing these important details on multiple levels of the organisation contributes the practical environment into factual insights on the current versus desired state. Figure 50 demonstrates the dashboards for all three organisational levels: Strategic, Tactical and Operational. Continuous compliance becomes increasingly relevant due to regulatory requirements. The artefact supports a continuous compliance PDCA approach.

So the answer to this question is dual. As the table below presents the solution to the problem, as well as the importance to the stakeholder are articulated but they stay behind with the practical environment:

CASE / ARTEFACT REQUIREMENT	ARTEFACT SOLUTION TO THE PROBLEM	WHY IMPORTANT FOR THE STAKEHOLDER?
1. Key BIS management information	A prioritised key set of BIS management information to use in a dashboard	Because it creates a mutual ground of knowledge, awareness and items to be managed
2. Key BIS Governance practices and KSF	A rigorously prioritised set of BIS governance practices to use as a (self) assessment for BISG measurement	Because it creates a mutual ground of knowledge, awareness and items to be governed (evaluated, directed and monitored)
3. Key BIS management interventions	A rigorously prioritised set of BIS management interventions to use as a (self) assessment for BIS measurement	Because it creates a mutual ground of knowledge, awareness and items to be managed and frequently measured
4. Insight into BIS metrics	A set of relevant metrics created by experts to measure and manage BIS	Because it creates a mutual ground of knowledge, awareness on metrics to consider when managing BIS
5. Use of existing management models	An alternative view on modelling, capturing and presenting strategic (cyber) forces	Because, strategic models such as Porter can help contemporary CI(S)O overcome the knowledge / jargon gap between the CI(S)O and its stakeholders, BoD, Executive management

The construction of several parameters in the artefact contributes to solving part of the main problem stated in Chapter 1 and answers the main research question in numerous ways.

RESEARCH DELIVERABLES

This Design Science Research project has been conducted in close co-operation with companies and educational institutions. This has resulted in the construction of an artefact with numerous functionalities and variable parameters that can assist in the goal-setting, design and implementation of increasing BIS maturity. The active involvement of stakeholders in finding solutions is advocated in DSR, and it has actually occurred in this research. Managers, CIOs, CISOs, IT Directors and CFOs have actively contributed to the construction of the MBIS artefact. Chapter 6 elucidates five primary functionalities of the artefact, each relating to our central research question and the objectives set prior to this research project. These primary research deliverables are:

- 1 a) Parameters, insights and viewpoints that form a conceptual framework for BIS, and influences the BIS maturity at management as well as governance level (Board of Directors) as well as insights into factors that influence the BIS maturity.**
- 1 b) A design artefact-tool that supports the administrative work (for measuring and reporting purposes), which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational) – using the parameters defined for reporting the BIS maturity of the organisation – to boards, owners and other stakeholders.**

A defined analysis method which enables knowledge sharing, consensus building on priorities, make decisions enables stakeholder engagement, contributes to the increase of awareness and enables reflection.

The core artefact functionalities derived from this research that relate to the problems from chapter 1 are;

1. To **identify and register relevant legislation and regulations**, and the **persons who are responsible and accountable**. This is increasingly desirable in the Netherlands in view of laws and regulations such as the Data Breach Notification Act (2016) and the proposed Cybersecurity Incidents Affecting Vital Services Notification Act⁴⁹. Assigning responsibilities and accountability is demonstrated in chapter 6.2.1 in Figure 53: Case 1: Demonstrating the policy setting and maintenance.
2. **Identifying the risk owners**, the measures that must be taken, and the owners of these measures. This functionality makes it possible to monitor and measure these factors continuously, and includes the corresponding burden of proof. This functionality offers users an integral management approach. Identifying and assigning the risk owners is demonstrated in chapter 6.2.1 in Figure 50: Case 1: Demonstrating the risk overview and risk indications.
3. **Planning and designing numerous organisational and technical assessments** at the levels of governance, management and operations, which are visualised in a **dashboard**. The dashboards are demonstrated in chapter 6.2.1 in figure "Demonstrate the dashboarding on Strategic level (Governance), Tactical level (management) and operational level". The numerous assessments are presented in Figure 71: Evaluation of the artefact: List of all the BIS assessments in the artefact.

The administrative tool enables the capturing, storing, interpreting, measuring and reporting of the current and desired state and explicate the steps to bring about the improvement. The artefact has the ability to use best-practice assessments, audits and questionnaires such as ISO, OWASP, NIST etc. By making use of industry bodies the artefact has the ability to catch up with changing technology and regulatory requirements as well as sophisticated cyber threats. Maintaining this yourself in any artefact is a cumbersome task. Community bodies such as NIST or ISF maintain their frameworks and standards with the latest threats and propose mitigating activities which can be adopted in the artefact. Bodies such as UCF⁵⁰ provide "feeds" to maintain artefacts.

By periodically collaborating with business, management, BoD and other relevant stakeholders, about captured facts, via GSS and by making use of the Information Security Management System (ISMS) capabilities within the artefact BIS can be practiced as a continuous management practice and not as an ad-hoc project. The collaborative approach

⁴⁹ Source: European Union regulation 910/2014 Directive 1999/93/EC, article 19 is effectuated via the guidelines provided by ENISA

⁵⁰ Unified Compliance Framework (UCF). The UCF's maintains a repository of all regulator and community frameworks and provides feeds towards tooling. The UCF site interfaces via Application Programming Interfaces and cover all topics from security and versioning through the various calls these tools will need to make to establish and maintain two way access to the UCF's information.

enables the awareness and continuous learning process and self-reflection of all stakeholders involved [9], [67].

- The possibility of **quantifying the current and desired situations** and a presentation of the
- steps that are necessary to bring about improvements. These steps can in turn be used as guidelines for BIS. Demonstrated in chapter 6.2.2 in Figure 62: Case 4 Demonstrating BIS improvements and periodically changes via the IRO.
- Various **benchmarking** capabilities, specific to the sector concerned, which offer the manager a **factually-based frame of reference**. Demonstrating fact-based evidencing is done in chapter 6.2.2 in Figure 61: Case 4: Demonstrating evidencing-functionality.

By doing this Business Information Security surpass the tactical IT management level and enables to involve the strategic level and reflect the latter with peers. Also regulators or supervisory bodies can benefit from this since there is little –actuarial- data on certain industries and their performance with regard to BIS. The collaborative process via GSS maximises knowledge sharing and awareness between any group about the necessary insights into the required tactical and operational facts. This also contributes the sense of urgency and insights into “actionable items”.

The research, construction, demonstration and evaluation have resulted in a set of instruments that offer evident practical added value for organisations, and which also have wider social and economic relevance. This set of instruments is an example of the value that can be created by applying the DSR method. The outcomes will assist company boards and managers to get a better grip on major security threats in the future.

8.2 RESEARCH CONCLUSIONS

The main conclusions of the research can be divided into two major parts. The conclusions we draw from the first two exploration phases (1) and the conclusions we draw based on the establishment of the artefact (2). The two of them constitute the major conclusions described in the last section of this section (3).

8.2.1 CONCLUSIONS ON THE EXPLORATION INTO THE CONCEPTUAL FRAMEWORK FOR BIS (1).

Although the research data doesn't show that board room involvement actually increases BIS maturity, this is also revealed by the feedback from practitioners during sessions and workshops. They observe acceleration in maturity once boardroom members show active engagement. This urges the empirical validation of the Governance index in Chapter 5. This more empirical testing is also emphasised by Workman [6] and Flores [9].

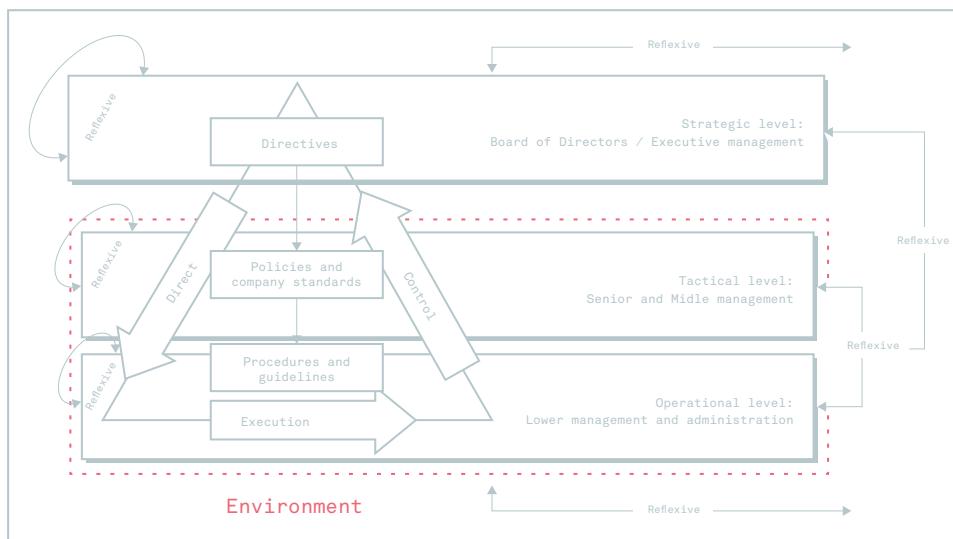


Figure 85: Direct Monitor and Control Cycle including reflection internally and externally.

In the initial explorative research project from Chapter 4 experts and target group respondents compiled a list of interventions. When validating the implementation of these interventions it was surprising that most of these interventions are not in place within mid-market organisations. They blame this to the absence of board and management involvement and clear guidance into laws and regulations. They raised the engagement of the board as top priority to increase the BIS maturity. The research also showed that 22% of the mid-market suggest that 'training and educate personnel on awareness' contributes most to security; this equals the opinion of experts according to the expert panel research. This urge of knowledge sharing in order to increase awareness is also mentioned by other researchers [1], [303], [68].

Also the filling in of the survey questionnaire has raised the awareness of mid-market participants. Responses to open questions such as "that's a good idea", "needs to be developed", "good idea to apply this" proved this and proofed the relevance of this research. One participant rose;

"Invest time to understand the language of the Board and identify where the IT risk may impact strategic business goals. While every company is different they are also very much alike. Sharing knowledge prevents re-invention 'of the wheel', will drive innovation and will it brings companies faster to a higher maturity level!"

The ultimately presented list of interventions form a frame of reference for mid-market organisations in order to practically increase business information security maturity. A carefully selected list of interventions present those interventions that are most effective and easy to implement for a market that, according to the performed survey, struggles with the enforcement of essential interventions. By making use of a combination of the ISO best practices and for example the COBIT maturity model organisations can have better insights into the interventions they have applied as well as those they need to apply in order to achieve a certain maturity level. In order to prepare organisations for attaining the maturing process the researcher proposes seven preconditions that organisations need to take into consideration. The established core set of interventions was set as requirements candidates into the artefact. The objective of this artefact requirement is to measure (take a photo) the current state on BIS (as is) and the desired state (to be), and map out the steps to take. The research project described in Chapter 5 was a multidisciplinary, multi-layered approach to GSS security research. As a result a highly significant core set of Business Information Security Governance and Executive Management practices could be established. A set of BIS-related Governance practices that was not compiled and published in the Body of Knowledge ever before.

The BISG top 22 practices to attain and maintain a certain level of Business Information Security Governance maturity is later on widely adopted by organisations. This practice-oriented research immediately contributed to organisations since the list can be adopted, communicated and reported on. The researcher proposes larger-scale, longitudinal research via this GSS SecuriMeter method to measure evolvement of certain organisations or industries on how they deal with Governance practices. This is why the BISG top 22 was integrated as a requirement into the MBIS artefact (detailed explanation in Chapters 6 and 7) and is subject to the collaborative process. In this way a socially justified method, due to team collaboration on a large set of predefined data (i.e. top 20) will “*encompass social and adaptable security methods that are rigorously developed along with practice*” [151]. The result of this research phase is the design of a governance framework to monitor, evaluate and direct business information security.

A conclusion of the explorations in Chapters 4 and 5 revealed little attention at the level of board of directors and executive management. Although practitioner's literature suggests that board attention is growing [9], [304], the factual data taken from the artefact reveal the opposite. The organisations under review are unable to identify essential interventions, such as executing business impact assessments, and struggle with insufficient knowledge and skills. On the other hand it could be argued that the artefact provided a more critical and realistic perspective on the state of their BIS maturity. However, in both cases the feedback and feedforward loop have been supportive in maturing BIS. On the basis of these findings, it can be argued that communication and reflection as visualised above between multiple business layers and their security has to be aligned. The raised set of core BISG practices was set as requirements into the artefact with the objective to measure the current state on BISG

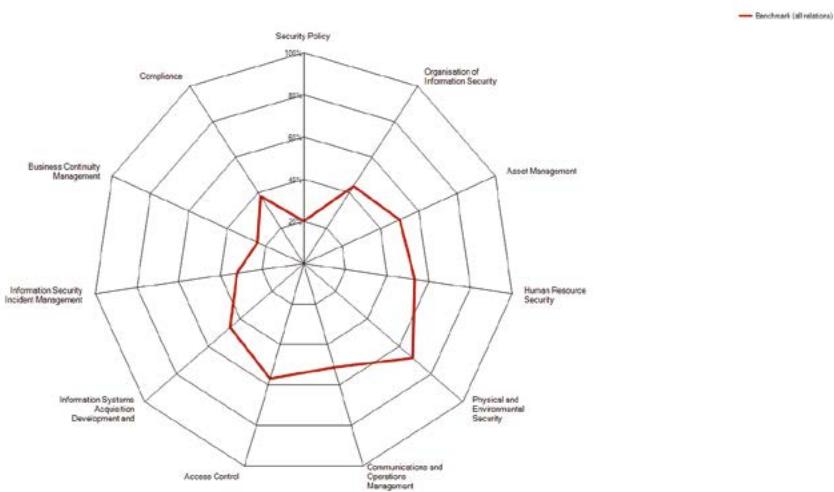


Figure 86: Spider diagram on the current status based on ISO27K (n=27).

(as is) and the desired state (to be), and map out the steps to undergo. I.e. solve the problem of low maturity in a straightforward and effective manner.

An important side effect of these two research phases was the new and fresh insights into BIS. The two established lists of practices and interventions called for numerous discussions, presentations, lectures and consultancy assignments. Over 100 organisations are being measured based on these methods. Important feedback that proof the relevance of this research; “*Organizations need to look at the higher scope of information security. They have to look for frameworks and approaches to assess measure and increase the effectiveness of information security in the organisation. Bobbert helps organisations measure and increase an organisation's maturity level relative to information security*” and “*The necessity of good information management is increasing to ensure business continuity. With that also the security of that information and the awareness of that IT is just one of the elementary parts. Yuri Bobbert shows with his research that good information security management is about people, starting at the top. Bobbert presents conclusions that are a must read for all business owners, managers and directors of mid-market organisations that do not address business information -security- management consequently on their agenda*”.

8.2.2 CONCLUSIONS ON THE ESTABLISHMENT OF THE DSR ARTEFACT (2)

According to the guidelines of DSR artefact establishment we thoroughly elaborated on the construction of the artefact. Both the technical and functional requirements are presented via numerous examples. The numerous methods used to establish the requirements resulted in interesting views. First of all the GSS sessions with the stakeholder group of CI(S)Os gave a good impression of core management information which the artefact needs to display in order to contribute to solving the problem i.e. the absence of core management information. The participants also raised that they have gained new insight and knowledge and appreciate the discussion and interaction with their peers. A predefined set of requirements was taken into development and evaluation via Chapters 6 and 7. The items that were raised and prioritised by the group can also function as parameters of control.

The Delphi research performed in order to gain metric data from experts delivered a huge amount of qualitative data. This data was categorised and formed a set of core metrics at the level of Governance, management and operations that contemporary boards can directly apply. By implementing these requirements in the artefact as measurement criteria (per level of maturity) enables organisations to have direct insight in factual data. The metric items that were raised and prioritised by the Delphi group can function as parameters of control.

Important feedback that proof the relevance of this research;

"I'm seeking for good security metrics because currently we only report on our known risks" and *"If I could had an answer to all these three questions. This is what I'm looking for."*

These last two remarks also show the necessity of this research and the exchange of these insights. It also shows the high level of engagement of security professionals to participate in scientific research.

Case 5 revealed two astonishing facts. First of all the fact that security professionals are not fully aware of the external influence that have influence in their security strategy. And second of all the respondents acknowledge that 58 percent consider it important addressing these external forces in their strategy formulation in the future. Since they did not do this up until the survey.

Therefore the result of this survey showed that new knowledge items gained via other models can help the security practitioner. The survey showed how the Five Forces can be subdivided into dynamic and static forces and how inadequate security strategy is, with its inordinate focus on static forces. The second important result from the survey showed that new knowledge item such as the five forces and the value chain model can be borrowed from Porter to enrich the current strategy formulation with in the BIS domain. According to the survey findings, security misses the mark, typically focusing on individual activities of the organisation rather than considering the role each activity plays in the wider picture. For

instance, security specialists see that their business has relationships with third parties, but seldom recognises these parties as potentially influential forces.

Understanding the value chain and the five forces is a prerequisite for business success. Yet, surprisingly, Porter's frameworks have yet to take hold in the BIS field, also proven by the outcome of the GSS session at the Erasmus University were all participants raised the use of Porters model as a potential successful parameter of strategising.

Integrating the knowledge items (such as Porters' Five Forces or Value Chain) into the DSR process enables the debate with in boardrooms on the scope and context of BIS. Integrating requirements such as the "Stakeholder analysis" into the artefact can also serve as parameters of control.

The validation process revealed a critical analysis on the artefact functionalities. This showed that the artefact embodied too much functionality that was used very little. This validation urged the researcher and the development team to prioritise and select functionalities that actually contribute to BIS maturity. *As a critical reflection towards the environment (organisations) is that the attention is paid by doing too much instead of doing the right things.*

8.2.3 SUMMARY OF THE CONCLUSIONS

Chapter 5 also reveals the "business requirements" of macro and meso-oriented knowledge (such as regulations, industry norms) gaining, capturing, sharing, and reporting (knowledge management items) within groups. This Chapter 5 also reveals the efficiency of GSS within boardrooms and management teams (relevance) and proposes GSS as an instrument to effectively process knowledge items and gain consensus on BIS strategy and maturity. The findings from Chapter 6 (Porter research) are typically knowledge items. These novel new insights into new models were shared in sessions and workshops [305] and contributed to new knowledge for the audience (rigour as well as relevance).

By the continuous measuring based on the rigour frameworks and norms, empirical data is collected. This data is used in contributing the rigour due to publications on new insights, preconditions, lessons learned, critical success factors and barriers.

The research facts show that best practices from several bodies (NEN, ISACA, NIST) are applied but do not have sufficient effect. Numerous reasons have been mentioned throughout this research. These bodies are not yet part of the design cycle but need to be part of it. They can learn lessons from the empirical data why these frameworks fail [3], [151], [5].

Due to regulations, evidence-based working [306] and integral management DSR appears to be an effective method to; articulate the business problem via the literature, discuss topics

and increase knowledge due to GSS and collect, measure, report data on BIS via the artefact. Conclusion is that DSR embodies all those perspectives.

Most of the participants from the environment acknowledged that the data from the design science cycle (e.g. artefact establishment) contributes to knowledge gaining and sharing, strategic forces, metrics, e.g. research data from Chapter 5. These knowledge items were not gained from the literature rigour but from the empiric.

8.3 RESEARCH RISKS AND LIMITATIONS

In this section I will address the multiple risks and limitations this research faced as well as the mitigating controls that were put into place to ensure replicability, independence and precision [77]. In the multiple individual studies a predefined frame of reference was used in the form of; ISO27000 in chapter 2, Governance practices based upon SPRM in chapter 5, artefact construction based upon the approach of Johannesson and Perjons [73] in chapter 6 and 7 and the ENISA criteria in the comparison study. These frames of references, together with the approach of multiple participants from multiple sectors to ensure validity, and the use of GSS to capture and record data complements the reliability of the entire research process. All sessions were; predefined with a clear agenda, moderated by an external and professional moderator, recorded on video or audio and structurally reported. By following the GSS sanity requirements for reliable expert panel research set by Hengst [115] this contributes independence and limits the influence from the researcher and increases the possibility of similar outcomes if this process was repeated.

Other academic principles Recker refer to are Credibility and Confirmability. Credibility (internal validity) refers to the fact if the researcher has substantiated his findings with sufficient evidence. Credibility in this comparison study is achieved through triangulation, maintaining a chain of evidence via; a research proposal, process reports, notes regarding decisions making throughout the process, audio and video footage and GSS Meeting reports. When implementing and maintaining a chain of evidence Confirmability (aka measurement validity) is realised. Recker states "*Confirmability suggests that qualitative research findings can be independently verified by outsiders in a position to confirm the findings (typically participants)*" for example via the appendices that encompass all the data, a list of participants and their characteristics, detailed process reports, meeting notes with decisions throughout the process, video presentations and GSS Meeting reports etc.

By publishing the majority of the research and the intermediate results in academic papers and conferences a scientific regulative cycle judged the latter on most of the above-mentioned items.

The main focus of this research was to examine and validate qualitative factors of influence and other practices that form parameters of control for boards and management. The

methods used were mainly qualitative methods. A limitation of this study is therefore the absence of statistical data and analysis. The objective of this research was to examine causes and explicate problems mainly via qualitative methods, and apply these qualitative methods to parameters of control such as questionnaires and survey lists that express answers e.g. observations as quantitative scores. Drawing generalizable conclusions from these scores is only possible when the sample size is large enough, and the sampling contains some form of independent observations, which means that the score of an individual case, e.g. a measurement of BISG maturity, is influenced by the score of others. If BISG maturity measurements are made in groups, for example in boards or management teams, the presence of other members of the group influences the outcome and the results might therefore not be independent. The independence assumption is important when applying statistical techniques. Kline [248] warns statistical researchers that "*scores from repeated measurements of the same case are probably not independent.*" Kline continues: "... if scores are really not independent, results of analysis that assume independence could be biased." Drawing generalizable conclusions from the data gathered via the measurements taken, with the SecuriMeter, is thus not feasible. A key objective of this research project was to establish the first iteration of an artefact that has the most relevant parameters that boards can take into consideration. These parameters change due to time, technology and business requirements and require constant assessment and alteration, preferably via a regulative design cycle. Again, the aim here is not, in this initial phase, to be mutually exclusive and collectively exhaustive but to initiate debate among stakeholders to examine and determine resolutions to the BIS problem (for example, the checklist-based assessments in Chapters 5 and 6). When this qualitative approach is further evolved via the rigour and relevance cycles and the data from the environment such as BISG scores are entered into the artefact, it becomes a knowledge base in itself. This thus allows quantitative analysis on the data gathered in later stages. When this data set becomes extensive enough, and represents a reasonable sample size, statistical analysis can be performed. Statistical inference could be subject to future research.

Since the field of BIS is complex, as explained by Abraham [80], little work has been done on transferring an empirical field of research into knowledge items such as practices and critical success factors [7], so such attempts are clearly necessary. As put forward in the previous section, quantitative methods can be used when larger data sets are available and data generalisability is possible, for example in the phase when macro level data from generic BIS interventions is gathered. This data can be replicated if the data analytics is performed with due care, especially since drawing generalizable conclusions from small samples influences the valid representation of the group and thus the external validity. As Kline argues about the characteristics of the observations in a certain sample: "*there is a limited guarantee that the characteristics of any particular random sample will match those in the population*" [248].

There is very few academic research performed among true board members [30], [7]. This research project is also limited into examining board room members. Although

the SecuriMeter artefact has been used in assessing organisations, and also board room members were involved, they did not agree to use the data for research purposes. UWV Chairman of the board Bruno Bruins agreed to use his name related to the BISG measurement I have performed with him, but did not allow to publicly disclose the outcome of the measurement.

Another limitation is time. This research is performed during the period 2010 to 2017. Even though, in the IS research field this is a long time it is still limited to 7 years. Since the emergence of the field and the swift dynamics one can also state that 7 years is a long time. Besides the limited number of academic publications on security failures this last decade (compared to other disciplines such as healthcare, aviation, automotive) the confidentiality and shame of incident sharing is still present. In all surveys, all participants, are very limited in sharing incident information or failures. Also in the GSS sessions I observed reservation to share too much detail that can reveal the weak points of the organisation. As mentioned in the above sections, the introduction of ISACS⁵¹, public reports such as Ponemon, [307], CSI [308] ENISA [309], NCSC, integrated reporting standards [92], Corporate Social Responsibility (CSR) [310] might bring more disclosure to this domain. This information sharing restraint is considered as a research limitation.

The artefact as presented in this thesis captures two forms of knowledge base items. First, new theoretical concepts such as the BISG maturity assessment established in Chapter 5, the MBIS maturity assessment established in Chapter 4 and the examples rose from numerous research methods in Chapter 6. These are *scientific driven* concepts scrutinised in the design cycle of the DS framework and incorporated in the artefact as working methods to solve practical problems. The other knowledge base items are items that rose from the *practitioner community*. Most of the times fairly well documented in the knowledge base, for example in ISO standards, NIST standards, or other forms of security community driven frameworks and practices. In Chapter 7, thirteen examples of practitioner-oriented alterations were raised and represent a fraction of all other working methods that were incorporated into the artefact during the years of construction. Due to the combination of academic and non-academic oriented working methods both scrutinised in the design cycle process, a rigorously developed artefact was established. One could argue that although the artefact is not purely derived from academia-related items, research institutions, universities are encouraged to contribute to the further development of the MBIS artefact. In this research project the pure scientific driven items into the artefact are from the researcher himself, this is a limitation in the sense that the artefact is not tested with other researchers/authors theoretical concepts. Although I as a researcher incorporated mechanisms to secure the objectivity and transparency of my research, I am aware of my own role and influence on my research. The way I have secured the objectivity of this research is by:

51 Information Sharing and Analysis Centres (ISAC's) are public-private partnerships which have been organised per sector. The participants exchange information and experiences about cyber security.

- Making use of the DSR framework of Johannesson and Perjons which prescribes clear steps and criteria throughout the process and enables transparency.
- Making use of numerous participants from heterogeneous organisations / professions.
- Recording the GSS sessions on video or audio (with permission of the participants).
- Publishing the research approach, findings and conclusion in peer-reviewed-journals during the entire research.
- Documenting the sessions (GSS Meeting reports) and documenting the artefact development process (e.g. via change logs, version documentation, backlogs, etc.)
- Making use of an external professional moderator during the performed sessions.

All of these measures, which are applied to ensure objective and reproducible research, are listed in the appendices. This can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

Another limitation of this research is the direct link between the research method outputs as direct input for the artefact. For example, the used method of Group Support System technology can generate items such as ontological knowledge on parameters (i.e. stakeholders, compliance, policy criteria, and business drivers) but remain in the GSS software. After the GSS session the data needs to be manually implemented in the SecuriMeter artefact. A limitation in this research but certainly a step forward in DS research would be that GSS is the initial interface for the SecuriMeter. Therefore ontological and epistemological challenges can be prioritised during the session and directly imported into the artefact. This direct link enables the researcher to directly import relevant parameters into the SecuriMeter and further fine-tune the artefact based on the situational requirements at the customer end. This option is examined and can be implemented via the XML connection between the two software tools⁵².

The entire research into MBIS was performed with mainly Dutch customers. All participants are located in the Netherlands. Due to the absence of a fair number of foreign organisations limits the generalisability of the findings.

In several IT Alignment studies the success or failure factor lies sometimes in centralisation or decentralisation function of the IT department [311], [312], [313]. This aspect is not examined in this study even though it plays a role in the level of security effectiveness. There is a limited amount of research performed in the difference between centralised and decentralised environments. This dimension is not taken into consideration during this research project but could be subject to further research into meso-level research.

In line with the centralised and decentralised discussion, outsourcing the organisations security capabilities is also out of scope in this research project. Compared to the Business and IT alignment phenomena were sourcing is a fairly examined topic [314], within the

52 This was examined based upon the SecuriMeter version 3 and Meeting Wizard GSS software. Not for other GSS software tooling.

information technology (IT) security domain this is also examined but mainly for the technology and services perspective [312]. Paans, Schinagel and Schoon put great effort in outsourcing or insourcing the Security Operation Centre (SOC) function of the organisation. The authors conclude that SOC capabilities can be outsourced or for effectiveness objectives integrated with other organisations in the form of specific collaboration such as forensics and pen testing (RijkSOCs) [315]. This "SOC sourcing" is limited to the IT part of the much broader domain of Business Information Security. Because of the broadness of this domain it seems obvious from a strategic perspective to outsource certain parts of the BIS function, an organisation will always be accountable for their own BIS maturity level and the level of control over this process. Due to the limited number of academic publications on sourcing this broader BIS concept and the fact that organisations hold an obligation of organising the BIS function and the how question is subordinate, it is left out of scope in this research project. Organising and contracting questions are obviously part of the strategy formulation and hold a direct relation to the organisation –resource- capabilities.

8.4 RESEARCH CONTRIBUTIONS AND ASSUMPTIONS

INFORMATION SECURITY AS A STRATEGIC UNIQUE SELLING POINT (USP)

During the research some participating organisations were inspired to view Information security as an element that creates value. For example, GGN Mastering Credit applied, together with the researcher, the COBIT framework to reach a maturity level of 3 out of 5. This enabled them to reach a BIS maturity level which was prescribed for financial institutions that are regulated by the Dutch Central Bank. According to Security and privacy Officer FV this achievement is in line with the overall GGN Mastering Credit business objectives, to be perceived as an integer and engaged business partners towards their customers. This maturity level in relation to an ISO27001 certification enabled GGN Mastering Credit to acquire new customers [316]. According to FV this gives GGN Mastering Credit a competitive advantage towards the competition, "*especially since customers increasingly demand a certain level of BIS from suppliers, this higher level of BIS maturity becomes a Unique Selling Point*" [316]. FV participated in a publication in the Finance and ICT magazine [317].

Linking business objectives towards Business Information security initiatives was also performed by Timeos, a Dutch mid-sized pension fund. The Security Officer RvE, and the researcher engaged into a small coaching project with the objective to help the security officer align the business objectives to the security goals. This exercise gave the Security Officer of Timeos the ammunition to present his security plan to the board and master the knowledge and jargon gap.

Linking business objectives towards security objectives also helped medical Institute Verbeeten to increase the overall value perception. The objective was to improve the Maturity of Business Information Security, specifically on the awareness of the employees. TT

(facility manager) managed to measure and monitor the employee awareness over a certain timeframe due to smart formulated indicators. By doing this the Institute was able to comply with the NEN7510 as well as the CBRN regulations which require employees to be aware of handling confidential medical data and certain toxic substances. According to TvdD; “*Our initial objective of improving the overall security awareness is achieved*”, she proceeds; “*by adopting awareness campaigns into the HRM cycle we enforce our employees to take notice of what taking care of confidential data is all about*” [318].

PGGM, a large pension fund, also acknowledges that BIS has an indirect influence on customer value perceptions. As WP stated in a mutual case description about the use of COBIT and ISO in order to improve the BIS maturity [319]; “*Customers require certification and expect a working Information Security Management system. Besides our customers, also our regulator DNB requires this*”. “*If we fail in information security and PGGM hits the news, that has a direct influence on our image and customer value perception*”.

These cases are published in the book “How save is my “share”? [320], that highlight the perspective value creating of Business Information Security. These cases are based on interviews with organisations that collaborated in this action research and have directly or indirectly applied the SecuriMeter artefact. We can conclude that customers never have a direct requirement for adequate information security but most of the time it is indirect. Customers expect a proper handling of their privacy or other confidential information. Organisations that do not take this into consideration might suffer the consequences of a withdrawal of trust and thus less business.

THE PROCESS OF VALORISATION

After five years of doing Design Science research into the process of Maturing Business Information Security, and five thousand research and development hours spend with a research team, the artefact was acquired by DPA Group, a publically listed company which could find added value in applying SecuriMeter in their consulting practice and sell licences to customers. To me this is a classic example of the valorisation process. Numerous business problems led to well-articulated questions that were adopted in scientific research at the University of Utrecht, Den Haag and Antwerp. The problems were articulated in research objectives that encouraged academic researchers to address the problem and solve it with the use of an artefact. The following academic publications contributed to the rigour [249], [321], [322], [185]. By mutually, science and business, developing artefacts and apply this into business consultancy is the classic example of valorisation and the spin-off process. Nlemvo examined and published “The four stages of the global spin-off process”. From his in-depth analyses of the research data he distilled four stages in the global process of valorisation by spin-off.

Stage 1: to generate business ideas from research. In this research five cases of business problems led to the creation of new consulting offerings, mainly assessments that were adopted in the artefact. And sometimes knowledge items that can be considered during the consulting process of data gathering, analysing, scenario-planning, presentation, reporting and advisory. A knowledge items that was raised was the use of existing management models (i.e. Porter's Five Forces model).

Stage 2: to finalise new venture projects out of ideas. After the initial proof-of-concept phase described in Chapter 6 the MBIS artefact intellectual property was described and claimed via legal documentation. Due to partially Government funding for Research and Development within the BIS area a part of the artefact development was financially secured. The additional funding was gained from customers paying for the consulting services that were carried out with the artefact. An additional business plan was developed on how to exploit the artefact (Selling, licensing, convert into services) [323] and additional growth money was attracted from the bank to overbridge the financing gaps that traditionally occur with start-up projects and inventions [324]

Stage 3: to launch spin-off firms from projects. According to Nleovo, "At the end of the second stage of the process, a new venture project should be ready. The third stage deals with the creation of a new firm to exploit an opportunity managed by a professional team and supported by available resources. These are the three key pillars of any entrepreneurial success". In this stage a dedicated internal team was appointed with the development, marketing and sales of the MBIS artefact. An advisory board was installed to function as feedback forum for the research and development planning. External expertise such as lawyers, telesales and marketeers were contracted to bring the MBIS artefact to the market. The initial launch of the public version was done on the MBIS event in Lent in June 2013 in the presence of Dutch Cybercrime coordinator Dick Schoof, Antwerp University professor dr. Steven de Haes and many network partners and customers. This active engagement of a network ecosystem contributes to a higher spin-off performance [325].

Stage 4: to strengthen the creation of economic value by spin-off firms. After five years of research and development of the MBIS artefact and two years of commercial exploitation with customers the MBIS artefact has limitations. The main limitation is scale. Scale in the number of potential customers but also the size of customers. Since 2013 the SecuriMeter was mostly applied into mid-market organisations throughout the Netherlands. Although the underlying technology is scalable towards enterprise environments the environment of further incubation was limited in resources, time and money. Due to the size of the company, therefore the acquisition by DPA was tactically well timed, especially to create this desired up-scale. DPA serves with 1200 employees numerous enterprise customers within several industries throughout Europe. This new soil provide three opportunities for future growth of the artefact, in revenue (selling more licences and thus further establishing the valorisation process) but also extract more research data that is collected during consultancy

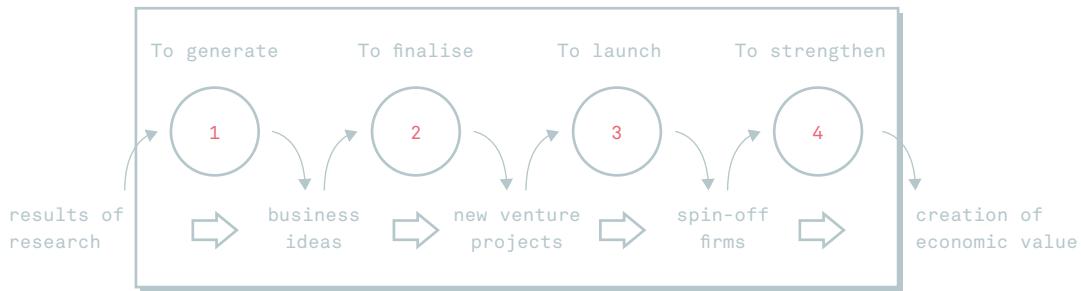


Figure 87: The spin-off process according to Nlemvo.

assignments. Data on maturity levels, critical success factors and best practices. This data can be processed anonymous for benchmark purposes and enables the design cycle to examine companies on a meso-level (over many industries) and macro level (over jurisdictions, countries and continents) to enable data generalisability.

8.5 FURTHER DEVELOPMENT OF THE ARTEFACT

In the figure below the maturity development of organisations is displayed. This Nolan and Norton model represents the evolution organisations go through. The curve represents a learning evolution through stages that depend on criteria that evolve over time. The assumption is that organisations and industries mature over time.

MICRO LEVEL (ONE ORGANISATION / SINGLE CASE)

At the micro level the rigour is contributed with one-dimensional details. Namely single case data taken for one organisation (relevance) with limited measurement methods (e.g. ISO27XXX, NEN). At the micro level lesson learned are drawn for the single organisation, however when in the design of the artefact industry statistics are included learned lessons can be evaluated. Relevance for one organisation is in practice measured on only a single case-based approach, and without an artefact which offers a longitudinal measurement, there is no support for a fact-based governance of the maturity of BIS. At the micro level the individual case finds its origin in a practical problem that's being dealt with due to literature research on a mainly operational level. There is no comparative material on a higher level of abstraction (industries, countries, etc.). This micro level remains isolated per organisation and thus limited in generalisability. Relevance is determined by the case study, for instance ISO27001, and 'compared' by the literature (rigour), however without 'a' securimeter, the measurements and governance of security (design), this remains a case-based approach which cannot be compared (benchmarked) on the level of industry (meso) or jurisdiction (macro).

MESO LEVEL (NUMEROUS ORGANISATIONS/BRANCHES)

The index gained in Chapter 5 is typically a macro level set of practices. The ISO based set of interventions from Chapter 4 can be applied on macro level within industries (NEN (health care) is based on ISO, BIR (Government) is based on ISO, BIWA (Water companies) is based on ISO, BIG (Local Government) is based on ISO etc. The other cases presented in Chapter 7 can typically be applied on macro level since they are generic (for example Cloud, BYOD, virtualisation etc.).

Chapter 4 reveals core interventions that can function as a cost-benefit analysis and prioritisation (business case management). Chapter 4 shows the cost-benefit of interventions. Once gathered, large longitudinal data with the ability to benchmark (at the intervention level and cost level) becomes relevant. Cost-benefit analysis is done by comparing numerous business case studies. The Integrated Risk Overview within the artefact makes it possible to address the cost per risk item and the benefit per control and therefore the ability to forecast trends or anomalies based on a set of comparable and longitudinal industry figures/data.

Within a chain of actors the artefact can measure and govern the security of the entire chain (stakeholder analysis). The artefact can contribute to the establishment of a stronger rigour regarding the facts. An industry norm can be evaluated by the artefact in the design cycle, which enables the early engagement of the stakeholder and positively influences the effect of the intervention [218]. An example of an industry norm is the NCSC web application security guidelines [326]. These new guidelines are based on the work of Tewarie [176] who also participated in the future development of the artefact to enable the IT Objective Maturity Model (ITOMM) measurement method in order to comply with the NCSC guidelines. Screenshots of this NCSC guideline within the artefact are enclosed in the appendix.

Meso-level deals with numerous organisations in certain industries. The rigour feeds the branch with best practices or generic branch interventions (such as PCI DSS for payment cards, HIPAA⁵³ and NEN for Healthcare etc.) in order to master a practical problem. The design cycle utilises the establishment of certain requirements such as NEN (via the use of a GSS method) within the artefact that measures MBIS within this industry. The current status within SecuriMeter is that industry measurement data is limited

MACRO LEVEL(ENTIRE SECURIMETER DATABASE/CROSS-INDUSTRY)

At the macro level organisations learn from previous gathered data, this contributes to solving knowledge problems. More data fuels the self-learning process of the organisation (relevance), the design science and the rigour.

Macro level deals with the highest abstraction level. This level is represented by micro data on individual organisations, data on industries and data of organisation across boundaries

53 The Health Insurance Portability and Accountability Act of 1996 (HIPAA was enacted by the United States Congress) requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. (source Wikipedia)

and jurisdiction. In order to achieve this, the relevance cycle needs to provide the design cycle with problems that require solutions that were validated in the rigour and deal with globalisation and other broader problems (cybercrime, espionage, state-sponsored attacks etc.). This information gained from the rigour can feed the design cycle with new requirements.

The future development of the industry as well as the artefact is typically subject to enhanced insights and requires an active, long-term commitment and engagement of Governing bodies (e.g. ISACA, NIST, ISO) academia and businesses to maintain the DSR cycle going and contribute to the overall maturing process of the BIS topic. Governing bodies should be part of the DSR cycle. The proposed fact-based DSR method can be part of the further development of international standards. These bodies (rigour) can learn from the empirical cycle. Further research on the application of DSR and the artefact into the proposed methodology is required. And as part of the DSR a continuous development of the artefact is also required. GSS can utilise the future functional and non-functional requirement setting, as well as the validation process.

Beyond monitoring and reporting towards the BoD and the organisations according to the selected requirements continuous further research need to be performed into bottlenecks, barriers and other influencing factors that limit the implementation. The artefact can be of assistance for the future research.

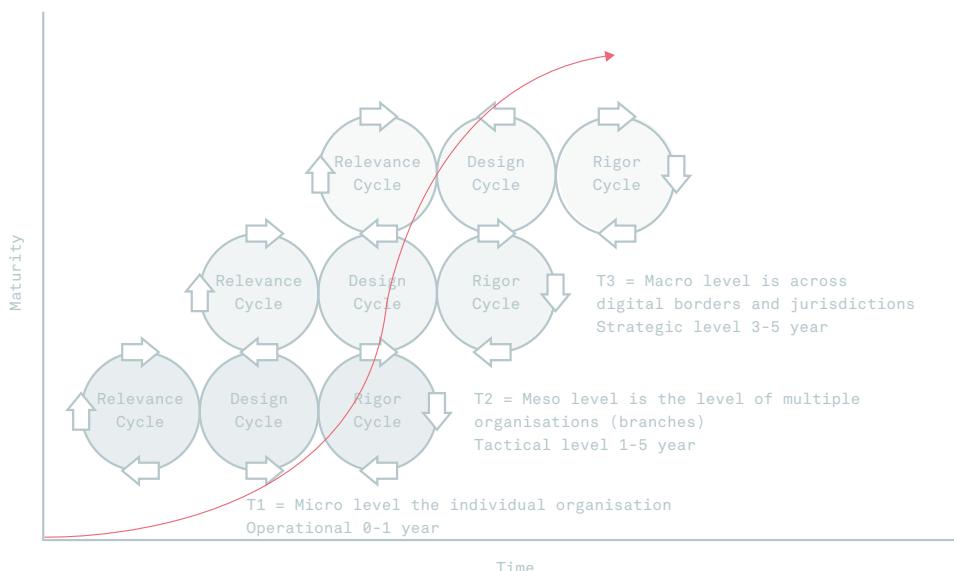


Figure 88: The artefact maturing process based on Nolan Maturity Model of Organisations.

Backlog of the artefact

The future requirements derived from the expert panel research in chapter 7 can function as a backlog of user stories for future development of the artefact. 16 items are not yet present but can be considered as a requirement and are potential backlog items that the developers can take into consideration for the next sprints. The top 5 is listed below.

NR.	ARTEFACT REQUIREMENT SUGGESTION SUBMITTED BY THE EXPERTS
1.	country of operation
2.	Translate known risks into costs of business discontinuity or lost opportunities
3.	security as part of KPIs, yearplan of employees
4.	available budgets
5.	look outside the organisation and learn from others their mistakes

DEVELOPMENT OF THE MATURITY CRITERIA WITHIN THE ARTEFACT

Tewarie [176] developed an Information security object repository. This repository encompass a comprehensive set of information security objects such as network, protocol, process, database, platform, mobile devices, connections, policies, storage, task and roles etc. This repository is theme based and therefore forms a structured method for measurement ad evidence collection. Audits and measurements can be performed based on these objects. Besides this self-assessments can be performed by organisations, due to NPLF classification of the objects. The sum of the individual object score, per theme, indicates the overall maturity level of the organisation. The pilot of this Information Security Object Repository (ISOR) within Information Security Object Maturity Model (ISOMM) is applied in the SecuriMeter as a pilot and seems promising for further research and action-based development.

REFERENCES

- [1] D. Feledi and S. Fenz, "Challenges of Web-Based Information Security Knowledge Sharing," in *Seventh International Conference on Availability, Reliability and Security*, IEEE, 2012.
- [2] R. Plasterk, "ICT beveiligingsassessments en Taskforce Bestuur en informatieveiligheid Dienstverlening," Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, 2013.
- [3] M. Siponen and R. Willison, "Information Security management standards: problems and solutions," *Information & Management*, no. 46, 2009.
- [4] D. Kluge and S. Sambasivam, "Formal Information Security Standards in German Medium Enterprises," in *Conisar*, Phoenix, 2008.
- [5] Puhakainen P and S. M., "Improving employees compliance through information systems security training; an action research study," *MIS Quarterly*, vol. 34, no. 4, pp. 757-78, 2010.
- [6] M. Workman, W. Bommer and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior*, vol. 24, no. 6, p. 2799–2816, 2008.
- [7] B. Lebek, J. Uffen, M. Neumann, B. Hohler and M. Breitner, "Information security awareness and behavior: a theory-based literature review," *Management Research Review*, vol. 12, no. 37, pp. 1049 - 1092, 2014.
- [8] W. Yaokumah and S. Brown, "An Empirical Examination of the relationship between Information Security / Business strategic alignment and Information Security Governance," *Journal of Business Systems, Governance and Ethics* , vol. 2, no. 9, pp. 50-65, 2014.
- [9] W. Flores, E. Antonsen and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Computers & security*, Vols. 2014-43, pp. 90-110, 2014.
- [10] J. Pfeffer and R. Sutton, "The Knowing Doing Gap: How Smart Companies Turn Knowledge into Action," no. Harvard Business School Press, 2001.
- [11] Ponemon Institute, "Business Case for Data Protection," Ponemon Institute LLC, 2009.
- [12] McKinsey, "Disruptive technologies: Advances that will transform life, business, and the global economy," The McKinsey Global Institute, 2013.
- [13] A. Dorri, M. Steger and S. J. R. Kanhere, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications magazine*, vol. 12, no. 55, pp. 119-125, 2017.
- [14] M. Conti, A. Dehghantanha, K. Franke and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF SCIENCE* , vol. 78, pp. 544-546, 2018.
- [15] C. Everett, "Social Media; Opportunity or risk," Computer Fraud Security, 2010.
- [16] Y. Jewkes and M. Yar, *Handbook of Internet Crime*, United Kingdom: Willan Publishing, 2010.
- [17] W. Fan and K. Yeung, "Online Social Networks - Paradise of Computer viruses," Science Direct, University of Hong Kong, 2011.
- [18] ITGI, "Information Risks; Who's Business are they?," IT Governance Institute, United States, 2005.
- [19] ISF, *Corporate Governance Requirements for Information Risk Management*, UK: Information Security Forum.

- [20] D. Hubbard, *The Failure of Risk Management*, Hoboken New Jersey: John Wiley & Sons, 2009.
- [21] C. May, "Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy," *Computer Fraud & Security*, Issue 5, 10-13, United Kingdom, 2003.
- [22] S. El Aoufi, "Economic Evaluation of Information Security," *Vrije University Press*, Amsterdam, 2009.
- [23] D. Ashenden, "Information Security management: A human challenge?," *Information Security Technical Report* 13 195-201, United Kingdom, 2008.
- [24] V. Solms, "From Information Security to business security," *Computer & Security*, Elsevier, South Africa, 2005.
- [25] V. Hooper and J. McKissack, "The Emerging role of the CISO," *Business Horizons*, vol. 56, no. Kelly School of Business, Indiana University, Elsevier, pp. 585-591, 2016.
- [26] K. Kobelsky, "A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-supported processes," *International Journal of Accounting Information Systems*, vol. 15, no. 4, pp. 304-322, 2014.
- [27] T. Neubauer and J. Heurix, "Defining Secure Business Processes with Respect to Multiple Objectives," in *Third International Conference on Availability, Reliability and Security*, Barcelona, Spain , 2008.
- [28] T. Neubauer, "Secure Business Process management: a roadmap, Reliability and Security," *International Conference* 20-22 April 2006, 2006.
- [29] A. Al-Omari, E.-G. O. and A. Deokar, "Information security policy compliance: the role of information security awareness," in *Proceedings of the American Conference on Information Systems*, US, 2012b.
- [30] U. Franke and J. Brynielsson, "Cyber situational awareness A systematic review of the literature," *Computers Security*, Stockholm Sweden, 2014.
- [31] COSO, "Where Board of Directors currently Stand in executing Their Risk Oversight Responsibilities," COSO, United States, 2011.
- [32] F. Dagblad, "ASML bevestigt hack," 2015. [Online]. Available: <https://fd.nl/economie-politiek/1094859/asml-bevestigt-hack>. [Accessed 2016].
- [33] Telegraaf, "UWV ontzettend laks met privacy," 04 December 2014. [Online]. Available: http://www.telegraaf.nl/binnenland/23409192/_UWV_laks_met_privacy_.html.
- [34] NOS, "Disruptions in Online Banking—377%," 2014. [Online]. Available: <http://nos.nl/artikel/618846-storingen-online-bankieren-377.html>.
- [35] FT.com, "Yahoo says executives knew about hack in 2014," 02 March 2017. [Online]. Available: <https://www.ft.com/content/88603346-feca-11e6-96f8-3700c5664d30>.
- [36] IEX.nl, "Hack on Gemalto has serious implications," 20 February 2015. [Online]. Available: <https://www.iex.nl/nieuws/ANP-200215-069/Hack-Gemalto-heeft-grote-implicaties.aspx>.
- [37] The_Washington_Post, "The Sony Pictures hack, explained," December 2014. [Online]. Available: http://wapo.st/1Allda1?tid=ss_mail.
- [38] NU.nl, "Belastingdienst had ernstig beveiligingslek," 4 March 2017. [Online]. Available: <http://www.nu.nl/politiek/4433631/belastingdienst-had-ernstig-beveiligingslek.html>.

- [39] Rechtbank van Amsterdam, "Gerechtelijke uitspraak Diginotar," ECLI:NL:RBAMS:2014:4888, 2014. [Online]. Available: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:4888&keyword=internet%20ontbreken..>
- [40] Forbes, "Target's CEO Steps Down, Company Shares Drop," <http://www.forbes.com>, United States, 2014.
- [41] NU.nl, "Yahoo-baas verliest miljoenenbonus na beveiligingslek," 04 March 2017. [Online]. Available: <http://www.nu.nl/internet/4507791/yahoo-baas-verliest-miljoenenbonus-beveiligingslek.html>.
- [42] L. Sandler and A. Tan, "Altegrity Files Bankruptcy After 'State-Sponsored' Breach," Bloomberg Business, <http://www.bloomberg.com/news/articles/2015-02-09/altegrity-files-for-bankruptcy-after-losing-vetting-contracts>, 2015.
- [43] Fox-IT, "DigiNotar Certificate Authority breach, "Operation Black Tulip"," FOX IT in assignment of the Ministry of the Interior and Kingdom Relations, Den Haag, 2011.
- [44] TWSJ, "Burglary Triggers Medical Records Firm's Collapse," The Wall Street Journal, 12 March 2012. [Online]. Available: <http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm's-collapse/>. [Accessed 12 2014].
- [45] S. Keller, A. Powell, B. Horstmann, C. Predmore and M. Crawford, "Information security threats and practices in small businesses," *Information System Management*, 2005.
- [46] WEF, "Partnering for Cyber Resilience; Risk and Responsibility in a Hyperconnected World - Principles and Guidelines," World Economic Forum,, Davos, Swiss, 2015.
- [47] B. Cashell, W. Jackson, M. Jickling and B. Webel, "The Economic Impact of Cyber-Attacks," Congressional Research Service, The Library of Congress, United States, 2004.
- [48] G. Walsh, V. Mitchell, P. Jackson and S. Beatty, "Examining the Antecedents and Consequences of Corporate Reputation: A Customers perspective," Britisch Journal of management; Blackwell Publishing LtD, UK, 2009.
- [49] F. Peters, Reputatie onder druk; Het managen van reputaties in een veranderende samenleving, Den Haag: SDU Uitgevers, 2012.
- [50] M. Ishiguro, H. Tanaka, K. Matsuura and I. Murase, "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market," Institute of Industrial Science, The University of Tokyo, Tokyo, Japan, 2011.
- [51] H. Cavusoglu, B. Mishra and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,," International Journal of E-Commerce, Dallas, Texas United States, 2-2002.
- [52] S. Von Solms and R. Von Solms, *Information Security Governance*, New York: Springer Science (ISBN 978 0 387 79983 4), 2009.
- [53] V. Solms, "From Information Security to Business Security," Computer & Security, Elsevier, South Africa, 2005.
- [54] J. Allen, "Governing for Enterprise Security (GES) Implementation Guide," Carnegie Mellon University, Software Engineering Institute, CERT , US, 2007.
- [55] IFAC, "Enterprise Governance: Getting the Balance Right," International Federation of Accountants, London, 2004.
- [56] ISACA, COBIT5 for Information Security, United States: ISACA , 2012.

- [57] R. Von Solms and B. Von Solms, "Information Security Governance; A model based on the Direct-Control Cycle," *Computers and Security* , vol. 2006, no. Elsevier Computers and Security 25, pp. 408-412, 2006.
- [58] M. Bevir, "Governance: A very short introduction," Oxford University Press., Oxford, UK, 2013.
- [59] C. Mallin, Corporate Governance, Third Edition, New York: Oxford University Press, 2010.
- [60] E. Koning and H. Bikker, "Using Standards to Create Effect in the Boardroom," *ISACA Journal*, no. 2, 2013.
- [61] M. Siponen, " An analysis of the traditional IS security approaches: implications for research and practice., " *European Journal of Information Systems*, vol. Sep 1, no. 14, pp. 303-15, 2005.
- [62] L. Sanchez, A. Santos-Olmo, E. Fernandez-Medina and M. Piattine, "Security Culture in Small and Medium Size Enterprises," *Communications in Computer and Information Science*, vol. 110, pp. 315-324, 2010.
- [63] A. Kankanhalli, T. Hock-Hai, C. Bernard and W. Kwok-Kee, "An integrative study of information systems security effectiveness," *International Journal of Information Management 23, Department of Information Systems, School of Computing, National University of Singapore,,* p. 139–154, 2003.
- [64] R. Flores and E. Antonsen, "The development of an instrument for assessing information security in organizations:Examining the content validity using quantitative methods," in *International Conference on Information Resources*, 2013.
- [65] W. Deming, "Elementary Principles of the Statistical Control of Quality," *JUSE*, 1950.
- [66] W. Tewarie, SIVA, Amsterdam: VU University Press, 2014.
- [67] J. Pai, "An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP)," *Management Decision*, no. Emerald Group Publishing Limited, 2006.
- [68] A. Veiga and N. Martins, "Improving the information Security Culture through monitoring and implementation actions illustrated through case study," *Computers and Security*, vol. 49, no. Elsevier Science Direct, pp. 162-176, 2015.
- [69] R. Moen, Foundation and History of the PDSA Cycle, Detroit: Associates in Process Improvement-Detroit, 2009.
- [70] J. Humble and D. Farley, Continuous Delivery, United States : Pearson Education Inc, 2011.
- [71] Solms von R. and Solms von B., " "Information Security Governance_A model based on the Direct-Control Cycle.," *Computers and Security. Science Direct.*, no. vol. 25. , pp. pp. 408-412 , 2006.
- [72] A. Volchkov, "How to Measure Security From a Governance Perspective , " *ISACA Journal*, vol. 5, 2013.
- [73] P.Johannesson and E. Perjons, An introduction to Design Science, Stockholm University: Springer, 2014.
- [74] A. Bryman and E. Bell, Business Research Methods, Oxford University Press: New York, 2007.
- [75] D. Silvermann, Doing Qualitative Research, London: Sage Publications, 2005.

- [76] M. Saunders and P. T. A. Lewis, *Research Methods for Business Students*, Essex England: Pearson Education Limited, 2007.
- [77] J. Recker, *Scientific Research in Information Systems*, Australia: Springer, 2013.
- [78] Ponemon, "2014 Cost of Data Breach Study: Global Analysis," Ponemon, 2014.
- [79] G. Dhillon and J. Backhouse, "Managing for secure organisations: a critique of information systems security research approaches," no. Information Security Research Centre, pp. 1-24, 1999.
- [80] S. Abraham, "Information Security Behavior: Factors and Research Directions," *AMCIS*, no. Proceedings of the Seventeenth Americas Conference on Information Systems, 2011.
- [81] P. Puhakainen, *A Design Theory for Information Security Awareness*, Finland: University of Oulu, 2006.
- [82] P. Spurling, "Promoting security awareness and commitment," *Information Management & Computer Security*, vol. 3, no. 2, pp. 20-26, 1995.
- [83] J. Spears and H. Barki, "User participation in information systems security risk management," *MISQ*, vol. 34, no. 3, pp. 503-522, 2010.
- [84] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture.,," *Decision Science*, Vols. 28-43, no. 4, pp. 615-60, 2012.
- [85] M. Kabay, "Using Social Psychology to Implement Security Policies," in *Computer Security Handbook, 4th Edition*, United States, John Wiley & Sons., 2002.
- [86] M. Siponen, "Critical analysis of different approaches to minimizing user-related faults in information systems security," *Information Management & Computer Security*, vol. 5, no. 8, pp. 197-209., 2000.
- [87] M. Siponen, "Neutralization: New Insights into the problem of Employee Information system security policy violations," *MIS Quarterly*, vol. 34, no. 3, pp. 487-502, 2010.
- [88] S. Pahnila, M. Siponen and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, Big Island, 2007.
- [89] A. Hovav and J. D'Arcy, "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea," *Information & Management*, vol. 49 , no. 2, pp. 99-110, 2012.
- [90] J. Dietz, *Enterprise Ontology*, Delft University: Springer, 2006.
- [91] E. Koning, "Assessment Framework for DNB Information Security Examination," De Nederlandsche Bank, Amsterdam, 2014.
- [92] PWC, "Integrated Reporting The Future of Corporate Reporting," PricewaterhouseCoopers AG , Germany, 2012.
- [93] J. Goo, Y. Myung-Seong and D. Kim, "A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate," in *46th Hawaii International Conference on System Sciences*, Hawaii, 2013.
- [94] A. Calder, *Implementing Information Security Based on ISO 27001 / ISO 27002*, Zaltbommel: Van Haren Publishing, 2009.

- [95] T. Haldin Herrgard, "Difficulties in diffusion of tacit knowledge in organizations," *Journal of Intellectual Capital*, vol. 1, no. 4, pp. 357-365, 2000.
- [96] I. Nonaka, "A Dynamic Theory of Organizational Knowledge Creation," *Organization Science*, vol. 5, no. 1, pp. 14-37, 1994.
- [97] I. Nonaka, K. Umemoto and D. Senoo, "From information processing to knowledge creation: A paradigm shift in business management," *Technology in Society*, vol. 18, no. 2, pp. 203-218, 1996.
- [98] S. Cook and J. S. Brown, "Bridging Epistemologies: The Generative Dance between Organizational Knowledge and Organizational Knowing," *Organization Science*, vol. 10, no. 4, pp. 381-400, 1999.
- [99] A. Fayolle, P. Kyro and J. Ulijn, *Entrepeneur Research in Europe*, United Kingdom: Edward Elger, 2005.
- [100] K. Golden-Biddle and K. Locke, "Appealing Work; An investigation of how Ethnographic Texts Convince," *Organisation Science*, vol. 4, pp. 595-616, 1993.
- [101] D. Tranfield and K. Starkey, "The Nature, Social Organisation and promotion of Management Research," *British Management Journal*, no. 9, pp. 341-53, 1998.
- [102] C. Hart, *Doing a Literature Review*, London: Sage, 1998.
- [103] B. Pfaffenberger, "The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing," in *Knowledge Technology and Policy*, Springer, 2000, pp. 78-92.
- [104] L. Festinger, "A Theory of Cognitive Dissonance," *Stanford University Press*, 1957.
- [105] S. De Haes and W. Van Grembergen, "Practices in IT Governance and Business/IT Alignment," *ISACA Journal*, vol. 2008, no. Information Systems Audit and Control Association., 2008.
- [106] H. T. M. Linstone, *The Delphi Method, Techniques and Applications*, New Jersey : New Jersey Institute of Technology, 2002.
- [107] R. Schmidt, K. Lyttinen, M. Keil and P. Cule, "Identifying software project risks: an international Delphi study," *Journal of Management Information Systems*, vol. 17 (4), no. 4, pp. 5-36, 2001.
- [108] C. Okoli and S. Pawlowski, "The Delphi method as a research tool: an example, design considerations and applications," *Information & Management*, vol. 42, pp. 15-29, 2004.
- [109] S. De Haes and W. Van Grembergen, "Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity," *International Journal on IT/Business Alignment and Governance*, Vols. January-March 2010, no. 1, pp. 14-38, 2010.
- [110] K. Maes, *The exploration of a process perspective on business cases and its relationship with the perceived success of IT enabled investments*, Antwerpen: University of Antwerp, 2014.
- [111] J. Rakhorst, "Thesis; Structures processes and relational mechanisms needed to formulate a good business information security strategy," Antwerp Management School, Belgium, 2013.
- [112] G. Vreede, D. Vogel, G. Kolfschoten and J. Wien, "Fifteen Years of GSS in the Field: A Comparison Across Time and National Boundaries," in *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, 2003.
- [113] Snel, J. Mulder and A. v. d. Niet, "Group Support Systeem: tactisch concept in," *Opsporing Belicht*, vol. Lectoraat Criminaliteitsbeheersing & Recherchekunde, no. ISBN 978-90-79149, in Dutch, Apeldoorn, 2011.

- [114] R. Newby, G. Soutbar and J. Watson, "Group Support System Approach," *International Smaal Business Journal*, vol. 21, no. 4, pp. 421-433, 2003.
- [115] D. Hengst, "Which facilitation functions are most challenging: A global survey of facilitators," Delft University of Technology, Delft, 2005.
- [116] E. Fern, "The Use of Focus Groups for Idea Generation: The effects of Group Size, Acquaintanceship, and Moderator on Reponse Quantity and Quality," *Journal of Marketing Research*, vol. 19, pp. 1-13, 1982.
- [117] S. Asch, "Effects of group pressure upon the modification and distortion of judgment," In H.Guetzkow (ed.) *Groups, leadership and men*, vol. Carnegie Press., p. Pittsburgh, 1951.
- [118] A. R. Dennis, J. S. Valacich and J. F. Nunamaker, "An experimental investigation of the effects of group size in an electronic meeting environment," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 20, no. 5, pp. 1049-1057, 1990.
- [119] H. T. M. Linstone, The Delphi Method, Techniques and Applications, New Jersey: New Jersey Institute of Technology, 2002.
- [120] D. Straus, How to make collaboration work; Powerfull Ways to Build Consensus, Solve Problems and Make Decisions, San Franciso: Berrett-Koehler Publishers Inc, 2002.
- [121] Delbecq, H. and A. Van de Ven, "A Group Process Model for Problem Identification and Program Planning," *Journal Of Applied Behavioral Science VII*, no. VII, pp. 466 -91, 1971.
- [122] J. Preece, Online Communities, England: Wiley and Sons, 2000.
- [123] R. Pols, Beïnvloeden en meten van Business and IT Alignment, Amsterdam: VU University Press, 2006.
- [124] Mulder et al., "New Applications of Group Support Systems," *Group Decision and Negotiation, University of Vienna, Austria*, 2005.
- [125] M. Turoff, "Social Decision Support Systems (SDSS)," in *Proceedings of the 35th Hawaii International Conference on System Sciences*, Hawaii, 2002.
- [126] M. Bieber, D. Engelbart, R. Furuta, R. Hiltz, J. Noll, J. Preece, E. Stohr, M. Turoff and B. Walle, "Virtual Community Knowledge Evolution," in *Proceedings of the 34th Hawaii International Conference on System Sciences IEEE PResS*, Washington DC , 2001.
- [127] A. Moorsel, D. Stepanova and S. Parkin, "A Knowledge Base for Justified Information Security Decision-Making," Newcastle University, New Castle, 2009.
- [128] J. S. R. Pfeffer, "The Knowing Doing Gap: How Smart Companies Turn Knowledge into Action," no. Harvard Business School Press, 2001.
- [129] A. Rutkowski, B. van de Walle and G. Eede, "The effect of Group Support Systems on the Emergence of Unique Information in a Risk Management Process: a Field Study," in *Proceedings of the 39th Hawaii International Conference on System Sciences*, Hawaii , 2006.
- [130] R. Yin, Case Study Research, Beverly Hills: Sage, 1994.
- [131] K. Eisenhardt, "Building Theories from Case Study Research," *Academy of management review*, vol. 14, no. 4, pp. 532-550, 1989.
- [132] D. Gioia, K. Corley and A. Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organisational Research Methods*, vol. 16, no. 1, pp. 15-31, 2012.
- [133] H. Miles, pp. 278-280, 1994.

- [134] Luft, J.; Ingham, H., "The Johari window, a graphic model of interpersonal awareness," in *Proceedings of the western training laboratory in group development*, UCLA , 1955.
- [135] J. Mason, Qualitative Researching, London, UK: SAGE Publications Inc, 2002.
- [136] R. Baskerville, "Distinguishing action research from participative case studies," *Journal of Systems and Information Technology*, vol. 1, no. 1, pp. 24-43, 1997.
- [137] R. Plutchik, "Foundations of Experimental Research," no. Harper's Experimental Psychology Series, 1983.
- [138] S. Hevner, J. March, Park and S. Ram, "Design Science Research in Information Systems," *Management Information Systems Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.
- [139] H. Rittel, "Reflections on the Scientific and Political Significance of Decision Theory." *The Institute of Urban and Regional Development*, vol. Working Paper 115, no. University of California, 1969.
- [140] J. Conklin, "Dialogue Mapping: Building Shared Understanding of Wicked Problems," no. CogNexus Institute, 2006.
- [141] H. Rittel, "On the Planning Crisis: Systems Analysis of the 'First and Second Generations,'" Institute of Urban and Regional Development University of California, Berkeley, California, 1972.
- [142] S. March and G. Smith, "Design and natural science research on information technology," *Decis Support Syst*, vol. 15, p. 251–266, 1995.
- [143] R. Wieringa, "Design science as nested problem solving," in *Proceedings of the 4th international conference on design science research in information systems and technology*, New York, 2009.
- [144] J. Nunamaker and M. P. T. Chen, "Systems Development in Information Systems Research," *Journal of Management Information Systems*, vol. 7, no. 3, pp. 89-106, 1991.
- [145] D. Arnott and G. Pervan, "How relevant is Fieldwork to DSS Design Science Reserach," IOS Press., Australia, 2010.
- [146] R. Wieringa, Design Science Methodology: For Information System and Software Engineering, Berlin: Springer, 2014.
- [147] M. Tremblay, A. Hevner and D. Berndt, "The use of focus groups in design science research," *Design Science Research in Information System Science*, vol. 22, pp. 121-143, 2010.
- [148] C. Argyris, "Double-Loop Learning,Teaching, and Research," *Academy of Management*, vol. 1, no. 2, 2002.
- [149] G. Kolschoten, J. Mulder and H. Proper, "De fata morgana van Group Support Systemen," *Informatie*, vol. 4, no. 5, pp. 10-14, 2016.
- [150] D. Whetten, "What constitutes a theoretical contribution," *Academy of Management Review*, vol. 4, no. 14, pp. 490-495, 1989.
- [151] M. Siponen, "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods," *Information and Organization* in press, 2005.
- [152] B. Wernerfelt, "A Resource based view of the firm," *Strategic Management Journal*, vol. 5, pp. 171-180, 1984.
- [153] J. Barney, "Firm resources and sustained competitive advantage," *Journal of Management*, vol. 17, pp. 99-120, 1991.

- [154] G. Kearns and A. Lederer, "A resource Based View of Strategic IT Alignment: How knowledge sharing creates competitive advantage," *Sciences*, vol. 35, pp. 1-29, 2003.
- [155] ISO/IEC27001, "Information Technology - security techniques - Code of Practice for Information Security Management," ISO/IEC, Geneva, 2005.
- [156] ISO/IEC27001:2013, "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements," ISO/IEC, Geneva, 2013.
- [157] P. Overbeek, M. Spruit and E. Lindgren, *Informatiebeveiliging onder controle*, Netherlands: Pearson Education Uitgeverij, 2004.
- [158] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," *IEEE proceedings of ARES*, vol. SecOnt workshop, no. Regensburg, Germany, 2013.
- [159] J. Christopher, Alberts and A. Dorofee, "OCTAVE Method Implementation Guide version 2.0," Carnegie Mellon University Software Engineering Institute, Pittsburgh, Pennsylvania, 2001.
- [160] G. Stonenburner, A. Goguen and A. Feringa, "NIST Special publications 800-27 Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, Gaithersburg, 2002.
- [161] ISF, "IRAM: Information Risk Assessment Methodology 2," Information Security Forum, <https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/>, 2016.
- [162] IIA, "Cybersecurity, What the board of directors needs to ask," The Institute of Internal Auditors Research Foundation (IIARF), Altamonte Springs, Florida, 2014.
- [163] M. Spruit and F. Noord, "Job profiles for information security; A basis for uniform qualification of professionals in information security," Dutch Society for Information Security (PvIB), Netherlands, 2014.
- [164] IPC, "Best Practices for Managing Information Security," IT Policy Compliance Group, US, 2010.
- [165] Accenture, "The Cyber Security Leap: From Laggard to Leader," Accenture, 2015.
- [166] A. Rose, "The CISO's Handbook — Presenting To The Board," Forrester, Cambridge, MA, USA, 2013.
- [167] COSO, "Leveraging COSO Across the Three Lines of Defense," The Committee of Sponsoring Organizations of the Treadway Commission (COSO)., United States, 2015.
- [168] R. Oyemade, "Effective IT Governance Through the Three Lines of Defense, Risk IT and COBIT," *ISACA Journal*, vol. 1, 2012.
- [169] K. Doughty, "The Three Lines of Defence Related to Risk Governance," *ISACA Journal*, vol. 5, 2011.
- [170] L. Greiner, "Evolution and Revolution as Organisations Grow," *Harvard Business Review*, 1998.
- [171] K. Ferraiolo en J. Sachs, „Distinguishing Security engineering Process Area's by Maturity Levels," Canadian Information Technology Security Symposium, 1996.
- [172] CMU, "Systems Security Engineering Capability Maturity Model (SSE-CMM)," Carnegie Mellon University , 1999.

- [173] N. Smit, "Business Continuity Management, A maturity Model," Erasmus University, Rotterdam, 2005.
- [174] D. Chapin and S. Akridge, "How Can Security Be Measured?," Information Systems Audit and Control Association Journal, Volume 2, 2005, United States, 2005.
- [175] S. AlAboodi, "A New Approach for Assessing the Maturity of Information Security," Information Systems Control Journal, ISACA, 2006.
- [176] W. Tewarie, Model Based Development of Auditing Terms of Reference: a structured approach to IT auditing, Amsterdam: VU Press, 2010.
- [177] ITGI, "COBIT Mapping: Mapping of CMMI for Development V1.2 With COBIT," IT Governance Institute, ISBN 1-933284-80-3, United States of America, 2007.
- [178] Gartner, "The Gartner Security Process Maturity Model," Gartner, United States, 2001.
- [179] Carnegie-Mellon, "Brief History of CMMI," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2004.
- [180] G. McGraw, S. Migues and J. West, "The Building Security In Maturity Model release 5.1.2," Creative Commons, 171 Second Street, California, USA, 2013.
- [181] Imperva, "Trends Report 2009," Imperva's Application Defense Center (ADC), United States, 2009.
- [182] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security," no. Elsevier, 2006.
- [183] W. Baets, "Some Empirical Evidence on IS Strategy. Alignment in banking," Information & Management 30 (4) 155-177, 1996.
- [184] N. F. Doherty and H. Fulford, "Aligning the information security policy with strategic information system plan," Computer & Security 25, Science Direct, United Kingdom, 2006.
- [185] Y. Bobbert, "Use of DEMO as a methodology for business and ICT Security alignment," Creative Commons, Nijkerk, 2008.
- [186] J. Luftman, "Assessing Business-IT Alignment Maturity," Communications of the Association for Information Systems, vol 4, art 14, US, 2000.
- [187] S. De Haes and W. Van Grembergen, "Enterprise governance of IT. Achieving strategic alignment and value," Springer, New York, 2009.
- [188] A. Silvius, Business and IT alignment in Context, Utrecht: Utrecht University, 2013.
- [189] P. Charantimatch, Total Quality Management, India: Pearson, 2006-2011.
- [190] W. Shewhart, Statistical Method from the Viewpoint of Quality Control;, Dover: Department of Agriculture, 1939.
- [191] D. Zitting, "Are You Still Auditing in Excel?," Sarbanes Oxley Compliance Journal, 2015. [Online]. Available: http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=4156.
- [192] A. Papazafeiropoulou, "Understanding Governance, Risk and Compliance Information Systems The experts View," *InfoSyst Front*, no. 18, pp. 1251-1263, 2016.
- [193] H. Mintzberg, "The Fall and Rise of Strategic Planning," Harvard Business Review, US, 1994.
- [194] B. Von Solms and R. Von Solms, "The 10 deadly sins of Information Security Management," Computers & Security, South Africa, 2004.

- [195] F. Sveen, J. Torresa and S. Sarriegia, "Blind information security strategy," *International Journal of Critical Infrastructure Protection* 2 95-109, Spain, 2009.
- [196] H. Ansoff, *Corporate Strategy; An analytical approach to business policy for growth and expansion*, New York: McGraw-Hill, 1965.
- [197] G. Westerman and R. Hunter, *IT Risk, Turning Business Threats into Competitive Advantage*, Boston MA: Hardvard Business School Press, 2007.
- [198] L. A. Gordon, M. P. Loeb and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?", *Journal of Computer Security*, vol. 19, no. 1, pp. 33-56, 2011.
- [199] L. Gordon, M. Loeb and T. Sohail, "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, vol. 34, no. 3, 2010.
- [200] S. Shackelford, "Should your firm invest in cyber risk insurance?," *Business Horizons*, no. Center for Applied Cybersecurity Research & Kelley School of Business, pp. 349-356, 2012.
- [201] Ponemon, "Perceptions about network security," Ponemon Institute, United states, 2011.
- [202] Y. Bobbert, "Sterke concurrentiekracht met gedegen IT risk management," *Finance & ICT Magazine*, vol. 14, p. 4, 2012.
- [203] H. Herath, "Cyber-Insurance: Copula Pricing Framework and Implications for risk Management," in *Workshop on the economics of Information Security*, Pittsburg, 2007.
- [204] F. Innerhofer-Oberperfler and R. Breu, "Economics of Information Security and Privacy," in *Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study*, Springer US, 2010, pp. 249-278.
- [205] N. Meulen, "Investeren in Cybersecurity," RAND Corporation, Santa Monica, Calif., and Cambridge, UK, 2015.
- [206] I. Ansoff, *From Strategic Planning to Strategic Management*, John Wiley & Sons Inc (June 1976), 1976.
- [207] A. Sohal and P. Fitzpatrick, "IT governance and management in large Australian organisations," *International Journal of Production Economics (Elsevier Science)*, vol. vol.75, no. 1, pp. 97-112, 2002.
- [208] ISACA, "Cobit5 Executive Overview "Optimise Your Information Systems; Balance Value, Risk and Resources," *ISACA*, p. 4, 2012.
- [209] ISACA, "An Introduction to the Business Model for Information Security," ISACA, United States, 2009.
- [210] S. Von Solms and R. Von Solms, *Information Security Governance*, South Africa: Springer, 2009.
- [211] R. Starreveld, H. de Mare and E. Joels, *Bestuurlijke Informatieverzorging*, ISBN 9014034822: Samson Uitgeverij, 1985.
- [212] M. Jensen and W. Meckling, "Theory of the firm: Managerial Behaviour, Agency Costs and Ownership Structure," *Journal of Financial Economics*, no. 3, 1976.
- [213] A. De Leeuw, *Systeemleer en organisatiekunde*, Een onderzoek naar mogelijke bijdragen van de systeemleer tot integrale organisatiekunde, Stenfert Kroese, 1974.
- [214] L. Donaldson and J. Davis, "Stewardship Theory or Agency Theory: CEO Governance and shareholder returns," *Australian Journal of management*, vol. 16, no. 1, 1991.

- [215] W. Van Grembergen, S. De Haes and E. Guldentops, "Structures, Processes and Relational Mechanisms for IT Governance," in *Strategies for Information Technology Governance*, US, Idea Group Publishing., 2004, pp. 1-36.
- [216] B. De Wit and R. Meyer, Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage 2nd ed, London: Thomson , 2005.
- [217] W. Van Grembergen and S. De Haes, Implementing Information Technology Governance; Models Practices and Cases, Hershey, United States: IGI Publishing, 2008.
- [218] T. Cummings and C. Worley, Organization Development & Change, Mason USA: Cengage Learning, 2009.
- [219] J. Porras and P. Robertson, "Organization Development Theory: A Typology and Evaluation," *Research in Organizational Change and Development*, vol. 1, pp. 1-57, 1987.
- [220] C. Cunningham, C. Woodward, H. Shannon and J. MacIntosh, "Readiness for Organizational Change: A Longitudinal Study of Workplace, Psychological, and Behavioural Correlates," *Journal of Occupational and Organizational Psychology*, no. 75, 2002.
- [221] T. Brown, "How to Mobilize the Executive Team for Strategic Change: The SFO Readiness Assessment," *Balanced Scorecard Report: Harvard Business School*, pp. 1-5, 2002.
- [222] E. Lawler and C. Worley, "Built to change," *Jossey Bass*, 2006.
- [223] B. Meyer and R. De Wit, Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage, London: Thomson, 2005.
- [224] R. Wieringa, Requirements Engineering: Frameworks for Understanding, Amsterdam: VU Press, 1996.
- [225] V. J. Aken and A. Nagel, "Organising and managing the fuzzy front end of new product development," in *ECIS working paper series; Vol. 200412*, Eindhoven: Technische Universiteit Eindhoven, 2004.
- [226] D. Ionita, J. Bullee and R. Wieringa, "Argumentation-based security requirements elicitation: The next round," *Evolving Security and Privacy Requirements Engineering (ESPRE)*, no. IEEE, pp. 7-12, 2014.
- [227] Y. Yu, V. Franqueirab, T. Tuna, R. Wieringa and B. Nuseibeha, "Automated analysis of security requirements through risk-based argumentation," *The Journal of Systems and Software*, no. 106, pp. 102-116, 2015.
- [228] V. Franqueira, T. Tun, Y. Yu, R. Wieringa and B. Nuseibeh, "Risk and argument: A risk-based argumentation method for practical security," in *19th IEEE International Requirements Engineering Conference (RE)*, Trento, 2011.
- [229] Gartner, "<http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses/>," Gartner, United States.
- [230] Deloitte, "Global Mobile Consumer Survey 2013; Divergence Deepens," Deloitte, 2013.
- [231] M. Silic and A. Back, "Shadow IT – A view from behind the curtain," *Computers & Security*, vol. 45, pp. 274-283, 2014.
- [232] Staten-Generaal, "Uitvoeringswet Richtlijn Jaarrekening," Eerste Kamer der Staten-Generaal, Den Haag, 2015.
- [233] G. Day, "Cybersecurity for Small Businesses," 23 October 2009. [Online]. Available: small-business.uk.reuters.com. [Accessed 29 January 2010].

- [234] Symantec, "Small Business Study," National Cyber Security Alliance, 2009.
- [235] R. Kuusisto and I. Ilvonen, "Information Security Culture in small and medium-sized Enterprises," 2003. [Online]. Available: http://www.academia.edu/1075891/Information_security_culture_in_small_and_medium_size_enterprises. [Accessed 26 July 2015].
- [236] J. Eloff and H. Venter, "A taxonomy for information security technologies," Elsevier, Pretoria SA, 2003.
- [237] ITGI, "Aligning COBIT 4.1, ITIL V3, ISO/IEC 27002 for business benefit," IT Governance Institute & OGC, United Kingdom, 2008.
- [238] E. Humpreys, "Information Security management standards: Compliancy, governance and risk management," Elsevier Ltd, Suffolk, United Kingdom, 2008.
- [239] B. v. Solms and S. Posthumus, "A framework for the governance of information security," Elsevier Ltd, South Africa, 2004.
- [240] ITGI, "CobiT: Governance, Control and Audit for Information Related Technology," 2000. [Online]. Available: www.itgi.com.
- [241] W. Grembergen and S. De Haes, "IT governance and its Mechanisms," ISACA, Antwerp, 2004.
- [242] R. Bojanc and J. Borka, "An economic modelling approach to information security risk management," International Journal of Information Management 28 (413-422), Ljubljana University, Slovenia, 2008.
- [243] K. Haufe, R. Colomo-Palacios, S. Dzombeta, B. Brandis and V. Stantchev, "Security Management Standards: A Mapping," *Procedia Computer Science* , vol. 100, pp. 755-761, 2016.
- [244] A. Moens, "Volwassenheid Informatiebeveiliging:Het 4 Aspecten Model," Platform van Informatie Beveiliging, Nijkerk, 2008.
- [245] J. Henderson and N. Venkatraman, "Strategic Alignment: Leveraging information Technology for transforming organisations," IBM System Journal, Vol 32, nr. 1, US, 1993.
- [246] B. Maizlish, IT Portfolio Management, New Jersey: Wiley, 2005.
- [247] B. v. Solms, "Information Security governance: Cobit or ISO 17799 or Both," Computers & Security, South Africa, 2005.
- [248] R. Kline, "Beyound significance testing," in *Statistics reform in the behavioral sciences* , Washington, American Psychological Association, 2013, p. Second Edition.
- [249] Y. Bobbert and J. Mulder, "A Research Journey into Maturing the Business Information Security of Mid Market Organizations," International Journal on IT/Business Alignment and Governance, 1(4), 18-39, October-December 2010, United States, 2010.
- [250] B. Von Solms, "Corporate Governance and Information Security," *Computers and Security*, vol. 20, pp. 215-218, 2001.
- [251] B. Von Solms and R. Von Solms, "From Policies to Culture," *Computers & Security* 23 (275-279), South Africa, 2004.
- [252] OECD, "The OECD Principles of Corporate Governance," Organisation for economic co-operation and development, Paris, France, 2004.
- [253] CACG, "Guidelines principles for corporate governance in the commonwealth; Towards global competitiveness and economic accountability," Commonwealth Association, Marlborough, New Zealand, 1999.

- [254] FRC, "Revised Turnbull Guidance," Financial Reporting Council, UK, 2005.
- [255] FRC, "The UK Corporate Governance Code," Financial Reporting Council, UK, 2010.
- [256] King, "King report on Corporate Governance for South Africa," King Committee on Corporate Governance, SA, 2002.
- [257] Bank for International Settlements, "Principles for enhancing corporate governance," Bank for International Settlements 2010, Basel Switzerland, 2010.
- [258] COSO, "Enterprise Risk Management Integrated Framework," September 2004. [Online]. Available: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf. [Accessed 22 10 2010].
- [259] COSO, "Embracing ERM, Practical Approaches for Getting Started," Committee of Sponsor-ing Organizations of the Treadway Commission, United States, 2011.
- [260] P. Weill and J. Ross, IT Governance, Boston Massachusetts: Harvard Business School Press, 2004.
- [261] CGTF, "The Corporate Governance Task Force Report, Information Security Governance: A CALL TO ACTION.,," National Cyber Security Summit, United States, 2004.
- [262] H. Kruger and W. Kearney, "A prototype for assessing information security awareness," Science Direct; Computers & Security 25 (289-296), South Africa, 2006.
- [263] M. Frigo and R. Anderson, "Embracing Enterprise Risk Management: Practical Approaches for Getting Started," 2011. [Online]. Available: http://www.coso.org/documents/Embracing-ERM-GettingStartedforWebPostingDec110_001.pdf. [Accessed 22 October 2011].
- [264] F. Conner and A. Coviello, "Information Security Governance: A call to action," The Corpo-rate Governance Task Force, United States, 2004.
- [265] B. Stackpole and E. Oksendahl, Security Strategy, Boca Raton Florida: Auerbach Publications, 2011.
- [266] A. Riabacke, "Managerial Decision-Making Under Risk and Uncertainty," *IAENG Interna-tional Journal of Computer Science*, Vols. 32-4, no. IJCS_32_4_12, 2012.
- [267] ITGI, Information risks; Whose Business are They, United States : IT Governance Institute, 2005.
- [268] P. Drucker, "Measuring Corporate Performance; The information Executives Truly Need," Harvard Business School, Boston, 1995.
- [269] R. Anderson, "Why information security is hard - an economic perspective," in *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, New Orleans, 10-14 Dec. 2001 .
- [270] K. Campbell, L. Gordon, M. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches; Empirical Evidence from the Stock Market," *Journal of Com-puter Security* 11 (3), United States, 2003.
- [271] A. Moens, "Volwassenheid Informatiebeveiliging:Het 4 Aspecten Model," Platform van Infor-matie Beveiliging, Nijkerk, 2008.
- [272] G. Montesdioca and A. Macada, "Measuring user Satisfaction with information security practices," *Computers and Security*, vol. 48, no. Science Direct, pp. 267-280, 2015.
- [273] NIST, "Directions in Security Metrics Research NISTIR 7564," National Institute of Standards and Technology , Gaithersburg, 2009.

- [274] J. Pironti, "Developing Metrics for Effective Information Security Governance," ISACA, US, 2007.
- [275] A. Jaquith, Security Metrics. Replacing Fear, Uncertainty and Doubt, US: Pearson Education, 2007.
- [276] A. Acquisti, A. Friedman and R. Telang, "Is there a cost to privacy breaches? An event study.," 2006.
- [277] M. Porter, How Competitive Forces Shape Strategy, United States: Harvard Business Review, 1979.
- [278] S. Schinagl and R. Paans, "A Vision on Risk-Oriented Education for Information Security Experts, Reducing System Language and System Thinking in 2020," in *HICSS*, Hawaii, 2016.
- [279] A. Vlist, "How do I get the mystic language of security experts in plain language?," 3 September 2015. [Online]. Available: <https://www.linkedin.com/pulse/hoe-krijg-ik-de-geheimtaal-van-security-experts-mn-aart-van-der-vlist>.
- [280] AberdeenGroup, "Best Practices in Security; Governance," Aberdeen Group, Inc. Boston, Massachusetts, 2005.
- [281] ITGI, "Information Security Governance, Guidance for Boards of Directors and Executive management 2nd edition," IT Governance Institute , United States, 2006.
- [282] C. Rossum, "Internetveiligheid hoort thuis in de Board Room," 24 Juni 2013. [Online]. Available: <http://ibestuur.nl/nieuws/internetveiligheid-hoort-thuis-in-de-boardroom>. [Accessed 2013].
- [283] A. C. Johnston and R. Hale, "Improved Security Through Information Security Governance," *Communications of the ACM*, vol. 52, no. 1, pp. 126-129, 2009.
- [284] Y. Jewkes and M. Yar, Handbook of Internet Crime, UK: Willan Publishing, 2010.
- [285] R. Peterson, "Integration Strategies and Tactics for Information Technology Governance," in *Strategies for Information Technology Governance*, Idea Group Publishing., 2003, pp. 37-80.
- [286] Forrester, "The Forrester Wave: Information Security and risk consulting services," Forrester Research , USA, 2010.
- [287] K. Golden-Biddle and K. Locke, Composing Qualitative Research, Thousand Oaks: SAGE, 1997.
- [288] C. Bruce, Research Students: Early Experiences of the dissertation literature review, *Studies in Higher Education*, 1994.
- [289] S. Chatterjee, S. Sarker and J. Valavich, "The Behavioral Roots of Information Systems Security_Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems*, , vol. 31, no. 4; ISSN: 0742-1222., pp. 49-87, 2015.
- [290] B. Lebek, J. Uffen and M. Breitner, "Employees' Information Security Awareness and Behavior; A literature review," in *2013 46th Hawaii International Conference on System Sciences*, Hawaii, 2013.
- [291] J. Brodkin, "12 biggest data breaches of the past 12 months," 29 10 2009. [Online]. Available: www.networkworld.com. [Accessed 2009].
- [292] RTL, "Disruption at ING Caused Hours of Unclearness About Account Balances," 3 April 2013. [Online]. Available: www.rtlnieuws.nl/nieuws/storing-ing-urenlang-onduidelijkheid-over-saldos. [Accessed 2014].

- [293] C. v. d. Lans, "Online Disruptions, Don't Lose Your Customers' Trust," 10 March 2014. [Online]. Available: www.usability.nl/2014/online-storingen-verlies-niet-het-vertrouwen-van-uw-klanten/.
- [294] NU.nl, "The Netherlands: Number One in Online Banking Disruptions," January 13 2014. [Online]. Available: www.nu.nl/tech/3674517/internetbankieren-relatief-vaak-getroffen-storingen.html.
- [295] TWSJ, "An inside look at companies in trouble from Daily Bankruptcy Review; Burglary Triggers Medical Records Firm's Collapse," Wall Street Journal; Bankruptcy Beat, 2012.
- [296] B. McBeath, L. Childs and A. Grackin, "Supply Chain Orchestrator - Management of the Federated Business Model in this Second Decade," <http://www.clresearch.com>, 2014.
- [297] G. De Vreede, R. O. Briggs, R. Van Duin and B. Enserink, "Athletics in Electronic Brainstorming; Asynchronous Electronic Brainstorming in Very Large Groups," *Proceedings of the 33rd Hawaii International Conference on System Sciences*, 2000.
- [298] G. Vreede, J. Boonstra and F. Niederman, "What Is Effective GSS Facilitation? A Qualitative Inquiry Into Participants' Perceptions," in *Proceedings of the 35th Hawaii International Conference on System Sciences*, Delft University of Technology Netherlands, 2002.
- [299] M. Ge and M. Helfert, "A design science oriented framework for experimental research in information quality," *Service science and knowledge innovation*, no. Springer, pp. 145-154, 2014.
- [300] R. Winter, "Design Science Research in Europe," *European Journal of Information Systems*, vol. 17, pp. 470-474, 2008.
- [301] J. Dietz and J. Hoogervorst., "The discipline of Enterprise Engineering," *International Journal of Organizational Design and Engineering*, vol. 3, no. 1, pp. 86-114, 2013.
- [302] A. Albani, D. Raber and R. Winter, "A Conceptual Framework for Analysing Enterprise Engineering Methodologies," *Enterprise Modelling and Information Systems Architectures*, vol. 11, no. 1, 2016.
- [303] J. Pai, "An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP).," *Management Decisions*, Vols. Jan 1-44, no. Emerald Group Publishing Limited, pp. 105-22, 2006.
- [304] CIGI, "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime," Centre for International Governance Innovation, 2015.
- [305] Y. Bobbert and A. Niet, "Cyber security in the boardroom," in *Oracle Innovation in Government Day*, Erasmus University Rotterdam, 2015.
- [306] J. Pfeffer and R. Sutton, "Evidence-Based Management," *Harvard Business Review*, no. January, pp. 1-13, 2006.
- [307] Ponemon, "When Trust Online Breaks Businesses Lose Customers," Ponemon & Venafi, US, 2015.
- [308] R. Richardson, "CSI Computer Crime & Security Survey," CSI, edition 13, United States, 2008.
- [309] ENISA, "Annual Report," European Union Agency for Network and Information Security, Greece, 2013.
- [310] A. Klaassen and H. Rijken, "RvC moet meer proactief 'mee ademen' met bedrijf," Grant Thornton, 11-2013.

- [311] P. Weill and M. Broadbent, "Improving Business and Information Strategy Alignment," *IBM Systems Journal* 32 (1) 162-179, US, 1993.
- [312] M. K. Khalfan, "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors," *International Journal of Information Management*, vol. 24, pp. 29-42, 2004.
- [313] G. Silvius, "Business and IT alignment in theory and practice," Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE Computer Society, 2007.
- [314] Derksen, Impact of IT Outsourcing on Business and IT alignment, Amsterdam: Vrije Universiteit; PhD Thesis, 2013.
- [315] K. Schinagl and K. Schoon, Security operations Center (SOC) Modelleren en meten van effectiviteit, Amsterdam: Vrije Universiteit, 2014.
- [316] M. Beelen, "GGN Behaalt ISO Certificaat informatiebeveiliging; Een referentiecase over GGN Mastering Credit," B-Able, Veenendaal, 2012.
- [317] Y. Bobbert and J. Mulder, "Sterke Concurrentiekracht met gedegen it risk management," *Finance & ICT*, 2012.
- [318] M. Beelen, "Security Awareness binnen instituut Verbeeten, van directie tot operatie; Een referentiecase over Instituut Verbeeten," DPA | B-Able BV, Veenendaal, 2013.
- [319] M. Beelen, "PGGM Waarbort privacy van 2.5 miljoen leden; Een referentiecase over PGGM," DPA | B-Able BV, Veenendaal, 2012.
- [320] Y. Bobbert, Hoe veilig is mijn 'aandeel?', Amsterdam: DPA | B-Able BV, 2014.
- [321] Y. Bobbert and J. Mulder, "Group Support Systems Research in the Field of Business Information Security; a Practitioners View," in *46th Hawaii International Conference on System Science*, Hawaii US, 2013.
- [322] Y. Bobbert and J. Mulder, "Governance Practices and Critical Succes Factors suitable for Business Information Security," in *International Conference on Computational Intelligence and Communication Networks*, India, 2015.
- [323] Y. Lee and R. Gaertner, "Technology transfer from university to industry: a large-scale experiment with technology development and commercialization," *Policy Studies Journal*,, vol. 22, no. 2, pp. 384-401, 1994.
- [324] R. Oakey, "High-technology New Firms. Variable Barriers to Growth," *Paul Chapman*, 1995.
- [325] A. Waltera, M. Auerb and T. Ritterc, "The impact of network capabilities and entrepreneurial orientation on university spin-off performance," *Journal of Business Venturing*, vol. 21, pp. 541-567, 2006.
- [326] NCSC, "ICT-Beveiligingsrichtlijnen voor Webapplicaties / Webapplication security guidelines," Ministry of Justice and Safety, The Hague Netherlands, 2015.
- [327] J. Thorp, "Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map," ISACA Journal, 2008.
- [328] M. J. Jacka and P. Keller, *Business Process Mapping: Improving Customer Satisfaction*, United States: John Wiley and Sons, ISBN: 978-0-470-44458-0, 2009.

ACKNOWLEDGEMENTS

DESIGN SCIENCE RESEARCH AS A DRIVER OF ARTEFACT ESTABLISHMENT

In order to emphasise my personal objective to make a concrete contribution, I describe the process of valorisation. All my working life I have been intrigued by people developing business opportunities based on scientific research. I have met numerous people who have done this. The first is Bob Jansen, the CTO and founder of RES software. His scientific study at Eindhoven University led to the development of virtual desktop software. I met Bob in 2013 in Den Bosch at his head office, when he was working on all kinds of projects linked to the scientific world. RES has become a market leader in virtualisation software worldwide. Another example of an inspiring researcher/entrepreneur is Dr Luc Brands. He developed his compliance software tool at the University of Eindhoven as part of his PhD research work. Nowadays this compliance software (BWise) is the world market leader in GRC tooling according to Gartner. BWise was acquired by NASDAQ. I met Luc in 2014. Dr Barry Derksen examined a huge number of organisations in terms of 'Business and IT alignment'. By doing this he developed a very effective working method, which he commercialised in the Netherlands. He grounded all his consulting working in scientific and non-scientific publications that gained enormous popularity among management readers. His book 'IT trends' is the best-sold IT management book in the Netherlands. Another international example is Dr Hsinchun Chen, who began developing COPLINK software in 1997. This software supports information sharing, analysis and visualisation of law enforcement data. COPLINK is now used in thousands of law enforcement agencies across the United States. Dr Hsinchun Chen continuously contributed academic rigour with publications and in parallel valorised the use of his software in companies. The objective of DSR is to create artefacts that can solve real problems and potentially create business opportunities, which lead to valorisation. According to Radboud University "*The goal of valorisation activities is to make concrete contributions to society, for instance in the form of exploration or evaluation activities as independent consultancy in industry.*"

In my opinion, this contribution to valorisation is one of the main reasons why Design Science Research is so popular among business researchers.

Applying theory in practical environments is a special experience. It encourages the intrinsic research passion. To do this numerous times is a present to each researcher. And to make it your profession is a privilege. My primary acknowledgement goes out to the organisations that were engaged in this process and therefore enabled the establishment of this special research project. Especially to all of those who were actively involved over the last 5 years and helped me in my research and establishing my own consulting practices based on the theoretical concepts of MBIS; Wim Plat, Hilko Batterink, Mariette Sjerp, Rene Munster, Frans Vrauwdeunt, Ronald Ferdinandus, Jan Willem Stuut, Wineke del Porto, Jan Just Keijser, Erik Wilms, Cor Brandenburg, Gerrit Dekker, Paul Boeijen, Tiny van der Klooster, Toon Trouw, Hans Ebels, Henk Pijp, Mattijs de Ruijter, Chris Alberda, Jeroen Kragten, Wim Pijnenburg, Victor Maassen, Klaas Kats, Jaap Okken, Jeroen van der Plank, Alexander Josiassen en Ronald van Erven.

The participants in 2010-2011; Sjoerd Ypma, Hans Admiraal, Herman Olde Heuvel, Walter Ligvoet, Robin Oomens, Jan Koen, Martijn Diersmann, Arno Verhofstad, Eelco Stieltjes, Paul Gijben, Raymond Schuiten, Wim Konings, Jeroen Hooft, Jeroen Buis, Laurens Hoppen, Maurice Vermeul, Joop Martens, Remco Oossenbrug, Maarten Boersma, Carlo Cammaart, Willem Stolk, Marc Claassen, Judith van der Sande, Onno Bult, Sahab Davoudi, Vincent Oosterhof, Rene Iriks, Frans Postma, Mike van Weerdenburg, Jan Ter Meer, Henk Shutte, Johan Steur, Jan Smits, Douwe Rijpstra, Edward Honkoop, Heidy driessens, Ruud Stroet, Hernany Hernandez, Laurens Sandifort, Rene Reith, Meine Hofman, Michel Blezer, Henk van Dijk, Bert Verlinden, Mattijs Ruyter, Erik Kamp, Bert Schipper, Jaap Booij, Hans de Moor, Thuy Tran Chau, Annemarie van Grunsven, Peter Klarenbeek, Oswald Veltman, Onno Bult.

The participants in 2012-2013 Daan Peters, John Geers, Gerard Ratering, Andrea Krusch, Arnoud de Vos, Frans van Kessel, Arie Linsen, Teun Tonino, Tom Bakker, Gerben Klein Baltink, Ard-Jan van Amerongen, Piet Kalverda, Arthur Donkers, Eric de Bruin, Kees de Brouw, Pascal Spoek, Lex Borger, Matthieu Bulkmans, Wim Zethof, aJan Willem Koopman, Bas Loen, Rik Looyestijn, Martin de Kok, Evelyn Coyer, Leon Kers, Peter Tak, Lars Klumpes, Alf Moens, Joop Schoppers, Peter Berndsen, Maarten Venhoek, Jan van den Berk, Robert Johan, Peter Bubberman, Evert-Jan Korving, Johan Rakhorst and Sjoerd Postuma for their support.

I would also like to acknowledge the employees of B-Able, and other people that inspired me in my entrepreneurial research work; Maarten en Toon Willems, dr. Joop de Jong, dr. Said El Aoufi, dr. Gilbert Silvius, Prof. Jan Hoogervorst, Prof. Jan Dietz, Prof. Steven De Haes, Prof. Wim van Grembergen, dr. Kim Maes, Prof. Boris Blumberg, dr. José Otte, Rene Wiersma, Edward van Dipten, dr. Marcel Spruit, Tsion Gonen, Robert Eman, Ben van Zuijlen, Andre Koot, Carla Smits-Nusteling, dr. Barry Derksen, Jan Koelewijn, Prof. Hans Mulder, Gillis Koomen, Erik Biekart, Paul van Noesel, Stefan Tezgel, Thomas Arends, Martijn Kok and my friends Wilco Blad, Robin van Dijk, Khaled Aziz, Rob de Waal for showing their interest.

Thanks to the people at UWV who facilitated me with making room for my PhD research and writing during my CISO ship; CIO Aart van der Vlist and Chairman Bruno Bruins. My CISO Office team members Cindy Kartoredjo, Carlo Seddaiu, Rob Roukens, Maarten Souw Maarten Baljon and Brenda Langedijk in offering me the opportunity to put my research work in practice. And the other people who directly or indirectly positively influenced the last year of writing Leo Benschop, Stef Schninagl and prof dr. Ronald Paans.

Thanks to the Nationale Nederlanden team; Amir Arooni, Dirk Brouwer, Nese Ozkanli, Marcel de Haan for making mutually drafting Figure 21.

Special thanks to the people who helped out with the extensive comparison study at the end of my PhD research project; dr. Jeffrey Pijpers, Kato Vierbergen, dr. Wiekram Tewarie, Rudrani Djwalapersad, Marc Vael, Rob van Diermen, Dr. Jan Hoogervorst, Ronald van Erven, Monique Neggers, Martin Knobloch, Jos Geskus, Bram Ketting

dr. Barry Derksen, Tony de Bos, Floris van den Dool, Rob Roukens, Joseph Mager, Mark Butterhof, Frank Mulder, Dennis Nuijens, Maarten van Dalen, Talitha Papelard, Jan Haro Wilbrennick, Toby Boerlage, Carlo Seddaieu, Maarten Souw, Daniel van Dorssen

A large number of people have helped in various ways with my research and writing this thesis. I owe the greatest thanks to those who read the manuscript or parts of it, looking for errors and obscurities; prof. Eric Verheul, dr. Barry Derksen, dr. Rob Pols, dr. Wiekram Tewarie, dr. Jose Otte, dr. Erik Poll, prof. Scapens, prof. Dries Faems.

Thanks to my initial promotor Prof. Wim van Grembergen. My main promotor; prof. Erik Proper, prof. Steven de Haes, and my dear friend and co-promotor prof. Hans Mulder

Finally I would like to thank my family; Nicole Mabel and Lolah Bobbert and my aunt Lola Bobbert for providing us with our "alternative house" and taking care of "my ladies" while I was writing. Lola showed real commitment and dedication to make my PhD work by providing my family with support and help. I also like to thank my aunt Pamela Bobbert in Canada who was always very interested in my PhD work but sadly past away during my writing. Finally I thank my father and mother Ronald and Carla.

INDEX

ISO15504 NPLF scaling	188	<i>Business requirements</i>	71
		BYOD Assessment	211
A			
Action Learning	33	C	
action oriented	41	Capability and Maturity Model (CMM)	59
Advanced Persistent Threats	128	Case Study Research	40
Antwerp Management School	314	Certified Ethical Hacker (CEH)	106
<i>Architectural requirements</i>	71	Certified Information Security Auditor	84
auditability	56	Certified Information Security Manager	84
Availability	56	Certified Information System Security Professional	84
		Chief Information Security Officer	56
B			
Bank for International Settlements (BIS)	104	COBIT5 for Information Security	71
benchmarking	215	Code Of practice (BS7799)	60
bias	36	<i>cognitive dissonance</i>	35
Big Data	16	collaborative research method	39
BIWA	268	Commission on Public Trust and Private Enterprise	104
BMIS		Commonwealth Association for Corporate Governance	104
The Business Model for Information Security	81	Communication Systems	39
Body of Knowledge	15	Confidentiality	56
Boeing Aircraft corporation (USA)	37	Confidentiality, Integrity and Availability (CIA)	56
Budget		Constructs	43
Barriers	90	continuous learning process	19, 256
Business Analysis Body of Knowledge (BABOK)	71	<i>contribution argument</i>	125
Business and IT Alignment (BITA)	70	Cookie assessment	211
Business Continuity Management (BCM)	59	credibility	42
Business Control Cycle	67	cross-sectional knowledge	40
Business Impact Analysis (BIA)	20	cyber forces	161
<i>Business Information Security Governance (BISG)</i>	66	Cybersecurity Incidents Affecting Vital Services Notification Act.	255
Business Information Security Maturity	58		
Business International Institute of Business Analysis	71		

D			
Dashboarding	214	Explicit Knowledge	33
Data Breach Notification Act	255	External interfacing	73
Data Layer	172	Extreme case studies	42
Data Leakage Prevention (DLP)	20	F	
Database Security assessment	211	Facetime	39
Decision Theory	39	Fear Uncertainty and Doubt (FUD)	35
Delphi Research	36	Financial Reporting Council (FRC)	104
Design Science Research	28, 42	financial reporting,	83
deterrence efforts or sanctions	30	Firewall Security Assessment	211
DigID Pre-Audit	211		
Diginotar	16	G	
Document generator	174	Gartner Hype cycle	126
Document management	216	generalisability	41
Document store;	217	Generally Accepted System Security Principles	
domotica	63	(GASSP)	118
DPA Group	314	geopolitics	51
Dynamic Systems Development		GGN Mastering Credit	265
method (DSDM)		Google+	39
E		Governance Risk and Compliance (GRC)	65
<i>Ease of implementation</i>	88	Governance, Delegation, Accountability and	
EDP auditing	83	Control	67
EDP Auditing perspective	84	Governance, Delegation, Accountability and	
EE Network	328	Control (GDAC) theory	163
<i>Effectiveness.</i>	88	Graphical Layer -	173
Interventions	88	Graphical User Interface (GUI)	168
ENISA	263	Greiner Growth Model	58
Enterprise Governance	17	group interaction	31
Enterprise Ontology	32	H	
Enterprise Risk Management Integrated		Health Insurance Portability and Accountability	
Framework	104	Act	
epistemological aspects	32	HIPAA	81
Erasmus University	224, 260	Hogeschool Utrecht	208

I			
Impairment Resources	16, 156	ISACA	63
Information Function (IF)	32	ISACA (Information Systems Audit and Control Association)	60
Information Security (IS)	15	<i>ISMS</i>	224
Information Security Forum (ISF)	18	ISO38500	68, 110
Information Security Governance Practices	105	IT Alignment and Governance Research Institute (ITAG)	314
Information Security Management System (ISMS)	78	IT balanced scorecard	109
Information Security Management System" (ISMS)	180	<i>IT Dependency.</i>	110
Information Security Object Maturity Model (ISOMM)	270	IT Governance Institute (ITGI)	17
Information Security Object Repository	270	IT Objective Maturity Model	268
Information Sharing and Analysis Centres (ISAC's)	263	IT Policy Compliance Group	56
Information Technology (IT) Security	15	IT Security Management	103
ING Bank instantiation	156 125	ITOMM	
Institute Verbeeten	265	IT Objective Maturity Model	268
Integrated risk overview	205	J	
Integrity	56	Johannesburg Stock Exchange	161
Interfacing Layer	173	K	
Internal Control Guidance to Directors, Turnbull Report	104	Key BIS management information	128
International Business Machines (IBM)	37	key performance indicators (KPIs)	157
International Federation of Accountants (IFAC);	17	King Report on Corporate Governance	161
International Organization for Standardization	78	Knowledge and Skills	
Internet of Things (IoT)	18	Barriers	90
Internet of Things,	16	L	
Internet Protocol (IP)	169	LAN vulnerability assessment	211
Interpretivism	29	Law enforcement	156
Intrusion Prevention Systems (IPS)	20	LDAP Integration	175
		Lean process improvement	19
		Lightweight Directory Access	
		Protocol (LDAP)	169
		Logic Layer	172

Loosen coupling	175	Operational Security Guidelines (OSG)	21
		Oracle	224
		organisational learning	33
M		<i>organisational membership</i>	39
machine-readable information security knowledge	39	<i>Organisational Structures</i>	105
Macro level	269	OWASP	200
Management and organisation	52		
<i>Management and peer influence</i>	31		
Meso level	268	P	
Michael Porter	154, 223	Partners in the (digital) chain	156
Micro level	268	PCI DSS	
Microsoft .NET 4.0 framework	167	Payment Card Industry Data Security Standards (PCI DSS)	81
mid-market segment	76	PDCA cycles	64
Multi Factor Authentication (MFA)	240	PDSA Plan-Do-Study-Act (PDSA)	65
Multiple case study	40	Perception and attitudes	90
		PGGM	265
		<i>plans, builds, runs and monitors</i>	66
N		plausibility	42
National Cyber Security Summit	105	practice	70
National Institute of Standards and Technology		predefined set of interventions	215
NIST	81	programme management	214
National Institute of Standards and Technology (NIST)	18	proof of concept (POC)	208
Nationale Nederlanden (Netherlands)	37		
Nominal Group Techniques	39	Q	
non-repudiation	56	Qualitative Research	28
NOVI University of Applied Sciences	314	Qualys Vulnerability Scanner	173
		quantitative research	28
O			
Objectivism	29	R	
OECD Principles of Corporate Governance		RACI matrix (RACI)	151
one-tier board	104	Radboud University's Institute for Computing and Information	
Ontological aspects	139	Sciences in Nijmegen.	314
<i>Operational level</i>	31	Relational Mechanisms	105
	17		

Reliability	41	Structures, Processes and Relational Mechanisms	71
Resource Based View	54	Structures, Processes and Relational Mechanisms (SPRM)	131
resource capabilities	52	<i>systematic literature review</i>	36
retrospectives	19	T	
RijkSOC	265	Tacit Knowledge	33
Risk assessment in Security		<i>Tactical level</i>	17
Argumentation	72	tame problems	43
S		Technical State Compliance	
SABSA	105	Monitoring (TSCM)	20
Secure Software Development (SSD)	20	The Dutch Policy Academy	37
SecuriMeter.Library.BE	172	The Enterprise Engineering Network	328
SecuriMeter.Library.BLL	172	The Hague University	213
SecuriMeter.Library.Util	172	The King Report on Corporate	
Security Alignment	63	Governance for South Africa	104
Security and Exchange Commission	104	Threat Intelligence (TI)	20
security by design	72	Total Quality Management (TQM)	60
Security Information and Event Management (SIEM)	20	Trade unions	157
Security Requirement		transferability	41
Lists (SRL)	21	trashbin check	128
Single case study	40	two-tier board	139
Skype	39	U	
Social Judgement	39	Unified Access Gateway (UAG)	169
Social Media Vulnerability Assessment	211	Unified Compliance Framework (UCF).	256
software as a service	167	Unified Modeling Language (UML)	163
speer phishing	128	Unique Selling Point (USP)	65
SPRM theory	71	University of Utrecht	266
SQL passthrough	175	<i>User (stakeholder) requirements</i>	71
SQL server	167	UWV	314
Stakeholder Analysis	205	V	
Stewardship theory	67	Validity	41
<i>Strategic level</i>	17	value chain	156

VHCD.Library.Database	172
Virtual Private Network (VPN)	169
Virtualisation Security Assessment	211
Vrije Universiteit	213
Vulnerability management (VM)	20
Vulnerability management assessment	211
W	
Web application vulnerability assessment	211
Web application Vulnerability assessment	211
WebEx	39
wicked problems	43
Wireless Vulnerability Assessment	211
X	
XBRL (eXtensible Business Reporting Language)	58

LIST OF ABBREVIATIONS USED

BABOK	Business Analysis Body of Knowledge	CSF	Critical Succes Factor
BCC	Business Control Cycle	CSR	Corporate Social Responsibility
BCM	Business Continuity Management	DDoS	Distributed Denial-of-Service (DDoS)
BCM	Business Continuity Management	DEMO	Design & Engineering Methodology for Organizations,
BETA	Binding Essence, Technology and Architecture	DNB	De Nederlandsche Bank (The Dutch National Bank)
BETA	Binding Essence, Technology and Architecture	DNS SEC	Domain Name System Security Extensions
BIS	Bank for International Settlements (BIS)	DSDM	Dynamic Systems Development method (DSDM)
BITA	Business and IT Alignment	DSR	Design Science Research
BoD	Board of Directors	EAL	the completion of Common Criteria
BoD	Board of Directors	EDP	Electronic Data Processing
BSC	Balanced Score Card	EE	Enterprise Engineering
CACG	Commonwealth Association for Corporate Governance	ENISA	European Union Agency for Network and Information Security
CC	Common Criteria for Information Technology Security Evaluation	FIPS	Federal Information Processing Standard
CEEN	CIAO! Enterprise Engineering Network (CEEN)	FRC	Financial Reporting Council (FRC)
CEH	Certified Ethical Hacker	GAAP	Generally Accepted Accounting Principles (GAAP)
CIAO	Communication, Information, Action, Organisation	GASSP	Generally Accepted System Security Principles (GASSP)
CISA	Certified Information Security Auditor	GDAC	Governance, Delegation, Accountability and Control
CISM	Certified Information Security Manager	GSDP	Generic System Development Process (GSDP)
CISSP	Certified Information System Security Professional	GSS	Group Support System
CITI-ISEM	Citigroup's Information Security Evaluation Model	GUI	Graphical User Interface (GUI)
CMM	Capability and Maturity Model	ICSA	International Computer Security Association
COBIT	Control Objectives for Information and related Technology	IEC	International Electro Technical Commission
COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO)	IFAC	International Federation of Accountants
		IP	Internet Protocol (IP)
		IRO	Integrated risk Overview

IS	Information Security	SaaS	Software as a Service
ISACA	Information Systems Audit and Control Association	SABSA	Sherwood Applied Business Security Architecture
ISC2	International Information Systems Security Certification Consortium (ISC) 2	SEC	Security and Exchange Commission
ISG	Information Security Governance	SOX	Sarbanes-Oxley (SOX),
ISMS	Information Security Management System	SPRM	Structures, Processes and Relational Mechanisms (SPRM)
ISMS	Information Security Management System" (ISMS)	SSE-CMM	Systems Security Engineering Institute at Carnegie Mellon University
ISO	International Organization for Standardization	TLS	Transport Layer Security
ISOMM	Information Security Object Maturity Model	UAG	Unified Access Gateway (UAG)
ISOR	Information Security Object Repository	UML	Unified Modeling Language (UML)
ITGI	IT Governance Institute	USP	Unique Selling Point (USP)
ITOMM	IT Objective Maturity Model	VPN	Virtual Private Network (VPN)
KPI	Key Performance Indicator	WAF	Web Application Firewall
LDAP	Lightweight Directory Access Protocol (LDAP)	WEF	World Economic Forum
NCSC	Nationaal Cyber Security Centrum	XBRL	eXtensible Business Reporting Language
NCSS	Nationale Cyber Security Strategie		
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid		
NIST	National Institute of Standards and Technology		
OD	Organisational Development		
OWASP	Open Web Application Security Project		
PCI DSS	Payment Card Industry Data Security Standard (PCIDSS)		
PDCA	Plan-Do-Check-Act		
PDSA	Plan-Do-Study-Act		
POC	Proof of Concept		
RACI	Responsibility, Accountability, Consulted, Informed (RACI)		
RISA	Risk assessment in Security Argumentation		

ABSTRACT

IT Security is becoming more complex and is changing more rapidly, and it has implications beyond the IT field, touching all the essential aspects of company operations. Since businesses increasingly rely on information and their supporting processes Information Security is more and more seen as part of Business Administration in close collaboration with key stakeholders that subsequently benefit the well-being of the firm. For this reason, we use the comprehensive term Business Information Security (BIS), which succinctly expresses the complexity and dynamic character of the field. The causes of the many security incidents that take place are very diverse, as are the strategies that have been chosen to keep them manageable.

The survey of the academic literature that was conducted for this thesis has shown that raising BIS maturity is not a technical matter that can be solved with systems and techniques; rather it requires a more sociological approach. The right attitudes, a certain kind of behaviour and the corresponding culture appear to be essential, and the tone set by senior management is also important in ensuring that BIS becomes part of integral management with an appropriate administration to support dialogues. In practice I observe companies struggling with excel and word documents scattered throughout the organisation with no single source of truth. This becomes even more challenging since we are entering an era where compliance and in "control statements" are a license to operate for firms. The main problem we aim to tackle in this research project on the one hand, to contribute to the required knowledge sharing, build the necessary consensus on priorities (where to start), make informed decisions and create the necessary engagement among stakeholders. In this thesis we refer to the collective term "Collaboration". And on the other hand determine the key concepts and practices that support the required analytical work and administration without reinventing the wheel. The main question we want to answer in this thesis is "*How can we establish a collaborative analysis method which utilises best practices for improving the maturity of BIS (MBIS)?*"

The first three chapters of the thesis outline the context for this study by providing an overview of the concepts that are most important for improving BIS. One important concept that makes it easier to recognise the diverse causes of problems is Design Science Research (DSR). DSR research focuses on developing and applying knowledge to support effective action in practice. This scientific knowledge does not supply ready-made solutions for specific problems; it is rather generic knowledge that professionals can use to design and develop specific solutions for specific problems (i.e. it is design-oriented). Beginning with this methodology, this study focuses on three essential areas and associated deliverables:

- **Examining the key concepts and parameters that influence BIS maturity.** The collective term parameter is used to capture terms such as interventions, barriers, practices, critical success factors, knowledge items and working methods that are part of the MBIS process. It is not intended to examine or scrutinise the current frameworks or models and the efficiency of these models.
- **Designing and building an experimental artefact** with relevant parameters. To contribute to capturing the above-mentioned items by constructing an artefact which has the initial relevant

requirements (parameters of control) needed to test these requirements and to demonstrate that it contributes to solving MBIS-related problems. I refer in this thesis to an artefact experiment.

- **Examining and defining a method** that addresses collaboration

Chapters 3, 4 and 5 focus on the development of this conceptual framework of parameters that influence BIS maturity. They give a qualitative picture of the most important concepts and interventions that managers can initiate to improve and maintain their BIS maturity. These interventions were first categorised and prioritised by experts on the basis of criteria such as ease of implementation and degree of effectiveness, and then validated by forty managers with experience in the field. This study has also identified seven critical constraints for efficient MBIS. These 'core interventions' and constraints are immediately applicable for organisations. One of the most important findings from the responses of these forty managers was the need for senior management to be engaged in the process of setting the BIS strategy (i.e. in setting the organisation's goals).

To analyse the failure of management to pay constant attention to improvement at all levels of the organisation (governance, management and operation), Chapter 4 describes an extensive literature study into diverse kinds of usable governance practices. Hundreds of sources in diverse locations across the world were consulted. The findings have been categorised, by means of a Group Support System (GSS) expert panel study, in the form of 22 essential governance practices and critical success factors. These essential practices and critical success factors can function as a conceptual BIS Framework of parameters for boards and senior managers.

In parallel with this academic research, hundreds of organisations have been helped to improve their BIS maturity on the basis of the core interventions from Chapter 3 and the core practices from Chapter 4. The practical experience gained in applying the scientifically generated knowledge of core interventions made us aware of the need for a set of instruments, an artefact that supports the analytical and administrative work to continuously monitor and measure the level of BIS maturity and to record the evidence. It would be a sort of book-keeping application for the head of the BIS Department, based on existing framework and practices.

Chapters 6 and 7 describe the design and construction of an artefact with the necessary parameters that were derived from chapter 3 and 4. These parameters had first to be translated into system requirements, both functional and technical. The particular contribution of DSR research is that it links the existing body of knowledge to actual practice and vice versa, in order to make the problems faced in practice more manageable. In the case of BIS, this involves a continuous interchange of knowledge so that the artefact itself is also constantly being improved.

To design the artefact on the basis of problems encountered in BIS practice, Chapter

6 describes five common problems found in practice. These five 'sore points' are very diverse – both in their causes and in their effects – and they manifest themselves at different levels in an organisation. These problems have been subject to a structured qualitative study and translated into functional requirements for the artefact, in such a way that the artefact can contribute to solving or more effectively managing a BIS problem. Chapter 6 then describes the design and construction of the artefact on the basis of Design Science Research.

Chapter 7 takes the same five problems as a starting point to demonstrate how the artefact works and how the requirements affect the span of control of the parties involved. This chapter also includes an evaluation of the performance of the artefact from various perspectives. Finally a comparison study among 38 experts was executed to demonstrated the working compared to a similar tool.

Finally, chapter 8 reveals the deliverables of this research being;

- 1 a) **Parameters, insights and viewpoints that form a conceptual framework for BIS,** and influences the BIS maturity at management as well as governance level (Board of Directors) as well as insights into factors that influence the BIS maturity.
- 1 b) **A design artefact-tool that supports the administrative work (for measuring and reporting purposes),** which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational) – using the parameters defined for reporting the BIS maturity of the organisation – to boards, owners and other stakeholders.

Resulting in a **defined analysis method** which enables knowledge sharing, consensus building on priorities, make decisions enables stakeholder engagement, contributes to the increase of awareness and enables reflection.

The five primary functionalities of the artefact, each relating to our central research question. These primary functionalities are:

- To identify and register relevant legislation and regulations, and the **persons who are responsible and accountable**. This is increasingly desirable in the Netherlands in view of laws and regulations such as the Data Breach Notification Act and the proposed Cybersecurity Incidents Affecting Vital Services Notification Act.
- **Identifying the risk owners**, the measures that must be taken, and the owners of these measures. This functionality makes it possible to monitor and measure these factors continuously, and includes the corresponding burden of proof. This functionality offers users an integral management approach.
- **Planning and designing numerous organisational and technical assessments** at the levels of governance, management and operations, which are visualised in a **dashboard**.
- The possibility of **quantifying the current and desired situations** and a presentation of

the steps that is necessary to bring about improvements. These steps can in turn be used as guidelines for BIS.

- Various **benchmarking** capabilities, specific to the sector concerned, which offer the manager a **factually-based frame of reference**.

These functionalities were validated by multiple expert panels and acknowledged the presence of these functionalities in the artefact. The outcome of the expert validation reveals that 91% of the relevant functionalities are designed and built in the SecuriMeter artefact. Thereby the artefact supports the collaboration to do the necessary analytical and administrative work to create one source of truth.

The main contributions and conclusions of this research are:

- A method that enables collaboration and administration to improve the Maturity of Business Information Security.
- A method that aligns business with information security and tested in practical environments
- An artefact that utilizes industry best practices and the required functionalities that contributes in the improvement of BIS
- An artefact that is proven by executing hundreds of measurements at 150+ midmarket and large organisations
- New insights in practices, enablers and critical success factors that maximise BIS and other academics to do further research on
- The gained research data enables future research in the MBIS field
- An improvement of the professional field of practitioner by providing research insights, data, findings

The artefact-tool that supports the administrative work has been applied in practice with more than a hundred organisations, using various methods from the existing body of knowledge plus the methods we have developed. In all more than 300 managers and IS professionals participated in the study. The outcome from more than 5,000 hours of work in research and development is a mature technology that has already been applied by diverse organisations. Just as there are levels of IS maturity within organisations – and the IS field is still maturing as a discipline – the artefact-tool will certainly mature further and pass through further necessary phases. One essential element will be the utilization of other methods found in the existing body of knowledge, such as international standards and frameworks. An important way to improve the artefact-tool is to further automate it so that the operational control effectiveness (BIS status) can be monitored and measured in real time. A built-in XML connector is a potential solution, and the first tests have been promising. Further automation and reducing the tolerances for error should contribute to higher reliability, so that management can approach their responsibilities – and legal liability – armed with good information. The continuous 'feedback learning loop' embodied

in Design Science Research offers a path of constant learning and improvement for the IS system, the organisation, and the communities that contribute to the developing body of knowledge.

This study has benefited from enthusiastic co-operation from many parties, who have demonstrated 100% willingness to participate in this and future research. The research has already led to several academic and practically-oriented publications. This Design Science Research has been conducted in close co-operation with companies and educational institutions. This has resulted in the construction of an artefact-tool with numerous functionalities and variable parameters that can assist organisations and can be used in further research.

CURRICULUM VITAE

Yuri Bobbert (1973) started his professional career in several business development and leadership positions in IT, at age 29 he established the company B-Able in 2003. Bobbert transformed his company from a fixed fee consultancy into a research-based consultancy firm, focusing on Design Science Research methodology (DSR). He actively combines his academic work with practical experience as a manager, constantly balancing academic rigour and practical relevance. In 2010 his research work resulted in his first book and the development of the SecuriMeter artefact, a dashboard application which assists organisations in improving their Business Information Security Maturity levels (MBIS). After ten years of leading B-Able, B-Able was acquired by DPA Group in 2014, a publicly listed company at the Amsterdam AEX. DPA moved forward based on the intellectual legacy of Bobbert and he served as a non-executive director of DPA, also starting the online platform mbis.eu, which consists of blogs, seminars and videos, etc. In 2014 he published his second book "How safe is my 'share'? (Hoe veilig is mijn 'aandeel')? With 25 practical case studies he reflects in this book on the security models used by B-Able and the problems that

were solved. In 2018 he published the book Critical Success Factors for the improvement of BIS together with Talitha Papelard Agteres. He is a frequent publisher in practitioner and academic literature.

In 2011 Bobbert became a visiting PhD researcher at Antwerp Management Schools' IT Alignment and Governance Research Institute (ITAG) and later on (in 2013) he extended his research work to Radboud University's Institute for Computing and Information Sciences in Nijmegen. In 2013 Bobbert became an Associate Professor (lector in higher education) at NOVI University of Applied Sciences in Utrecht. Since 2012 Bobbert is the chair of the LOI University of Applied Sciences Bachelor IT program supervising board. In 2016 Bobbert became lecturer at Antwerp Management School and promotor of Master students at several universities.

Bobbert currently serves as Chief Information Security Officer (CISO)) at NN-Group, an international financial institute. Prior to NN-Group he served as an interim CISO at UWV. In both positions he is able to put his research work into practice.



APPENDIX INDEX

APPENDICES THAT ACCOMPANY CHAPTER 1

National Cyber Security Centre (NCSC) letter on security breaches (Meldplicht en interventiemogelijkheden), European Security Breach Notification. This letter describes the directives for vital sector companies to adhere to the data breach notification act. Published in July 2012 in the Netherlands.

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 2

IN DIGITAL ARCHIVE:

Publication: This publication is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This paper focusses on the several research methods used and prescribes a Design Science Research approach for the development and implementation of the Artefact. Title: On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering in International Journal of IT/Business Alignment and Governance Volume 8 ♦ Issue 2 ♦ July-December 2017 (14 pages)

DOI: 10.4018/IJITBAG.2017070102

Publication: This publication is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This publication describes a literature review and comparison between research methods for designing and engineering a Business Information Security (BIS) artefact. Defining research methods to establish artefact functions (e.g. dash boarding, risk register) that reflect the parameters of control for Board of Directors, is the main goal. Finally a research method is proposed that was used in the thesis which can be used to establish an experimental dashboard with initial parameters of control. This research approach is based on a Design Science Research (DSR) approach.

DOI: 10.4018/IJITBAG.2017070102

Poster Publication: This publication is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS)". In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security

levels. This poster publication was used to present the research methods and approach of the thesis at the Enterprise Engineering Working Conference (EEWC) Forum in 2017 in Antwerp, Belgium on 9 - 11 May 2017. It visualises the DSR approach used in this thesis and the deliverables of the thesis in terms of papers and artefact functions.

url; <http://ceur-ws.org/Vol-1838/>

The appendices are accessible via the Radboud University digital archive, structured per chapter. And can be accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 4 IN APPENDIX DOCUMENT

List of preselected interventions e.g. first selection for setting the GSS agenda. These interventions were preselected by the expert based upon the relevance and applicability as an intervention for mid-market organisations.

Objectives of Expert Group Discussion, send by mail prior to the session. This document sets the objectives and expectations for the participants of the GSS session and is send by mail upfront to the participants of the GSS session.

Expert panel introduction presentation (PDF). This presentation provides an introduction for the GSS session. It provides context for the participants and sets the expectations on what is expected from the expert participants.

List of Expert Supplementation of security interventions. These interventions were raised by the experts during the GSS session.

Market definitions according to Gartner and CBS. These are mid-market definitions according the Centraal Bureau Statistiek (CBS) in The Netherlands and Gartner Research institute.

Maturity models. An overview of maturity models used in Information Security

Simplified COBIT information security maturity levels, source ISACA.

Ease of implementation BIS Interventions according to experts displayed in the graph

Effective Interventions Graph. A visualisation on the core MBIS interventions scored by the expert panel and ranked on the effectiveness.

E-mail invitation to the participants and web survey screenshots. These screenshot represent

the invitation for participants of mid-market organisations to join in the survey and displays the survey portal. The survey was held in Q2 2010.

List of the Participating mid-market organisations. This list displays the names of the companies who have participated in the survey. They agreed in disclosing their company name and keep their participants name confidential.

IN DIGITAL ARCHIVE

GSS Expert panel introduction Presentation. This presentation document is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS)". In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This presentation was given as an introduction to the GSS expert panel participants who were asked to pre-select and prioritise the core interventions for mid-market organisations that can potentially function as parameters of control in this experimental artefact. This GSS Expert panel session was held as the first of several other GSS sessions to establish the artefact requirements. This session was held at 15 February 2010 in Fort Vechten Utrecht and was recorded and documented in a separate Meeting report.

GSS Expert panel data in Meeting report in separate PDF. This dataset is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS)". In this research a Design Science research an artefact was established to measure, monitor and report how organisations can improve their Business Information Security (BIS) levels. This report reflects the entire Group Support System (GSS) research results that was collected during the session among 6 security experts. Objective of this expert panel research is to prioritize security interventions that contribute in the improvement of BIS maturity. The experts ranked the interventions on: a. Ease of Implementation and b. Effectiveness of the intervention. The report reflects the numeric scores as well as the graphs per intervention. Multiple disciplines participated in this panel session: Security manager, Auditor, Security Officer, consultant, accountant and lector. To support the expert panel research process we used a Group Support System (GSS). After this expert session surveys (questionnaire) with limited questions is composed and send out for feedback to mid-market organizations. In the form of a questionnaire the core interventions are presented and mid-market security/it managers needed to rank the most practical ones in order to increase their own BIS maturity levels. This will lead eventually to a framework with requirements, based upon a maturity model, of core interventions which can function as artefact requirements. This session was held on 15th February 2010 from 14.00-18.00 in Fort Vechten in Utrecht (Netherlands). During this 4 hour sessions the participants were asked to provide input to establish a core set of interventions which can be used for the improvement of BIS. This session was moderated by a professional moderator.

Video footage of the GSS Expert panel session held at 15 February 2010 in Fort Vechten Utrecht in separate MPEG available by the researcher and not in the archive. During this 4 hour sessions the participants were asked to provide input to establish a core set of interventions which can be used for the improvement of BIS. This session was recorded with permission of the participants and moderated by a professional moderator.

The survey data in the Excel file is displaying all the survey data that was collected in Q2 2010 by Dutch mid-market organisations. It consist of survey data on all core interventions according to the mid-market participants, percentages on interventions according to the survey results, scores of BIS barriers etc. The fields marked in red are the high scores compared to the rest. Table G to V reflect the core interventions the participant can score with Yes or No (if implemented), tables W to AL reflect the argumentation on the No if certain participants answered that a certain intervention was NOT implemented. The empty fields from tables W to AL therefor reflect a YES on the question. The latest column (AP) is the intervention suggestion mid-market participants rank as top interventions for mid-market organisations. The second excel tab reflect the scores in graphs.

Publication in International Journal of IT/Business Alignment and Governance (IJITBAG) 1(4), Page 18-39, in December 2010 under the title A research journey into Maturing the Business Information Security of Mid-market organisations in separate PDF. This publication is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This publication describes the literature review, expert judgement via GSS and mid-market validation of a core set of interventions that mid-market organisations can take into account for improving their BIS. The final core set of interventions are set as artefact requirement candidates in a later stage of the research.

DOI: 10.4018/jitbag.2010100102

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 5 IN APPENDIX DOCUMENT

Agenda for the Expert Panel session held at 25 February 2012 in Veenendaal

Governance practices literature list. This list contains a consolidated view into the top ranked practices and with their variance. The items are enumerated via: First the Discipline, the SPRM mapping, the main description of the practices, a detailed description of the practice,

the source of the practice and the extraction date.

Presenting the research paper on chapter 4 at the Hawaii International Conference of System Science (HICSS)

Presenting the research paper on chapter 4 at the ISACA conference (picture)

IN DIGITAL ARCHIVE

Literature Overview of all Governance practices sources before the GSS session. This dataset is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This data set was collected over a 2 year timeframe 2010-2012. This Excel file displays all the collected and examined sources on Governance practices in general that can form a reference for the GSS session. In this document you will see per tab the discipline (Corporate Governance (CG), IT Governance (ITG), Risk Governance (RG) and Information Security Governance (ISG). Row A represents the discipline of the practices, row B represents the mapping on SPRM to later on derive a clear list based upon Structures, Processes and Relational Mechanisms (SPRM), row C the description of the practice, row D a more detailed description and row E reflects the source of the practice in the literature. The tab cumulating represents the entire list of Governance practices that can function as input for the following GSS session with expert judgement.

Scores on BIS Governance practices after the expert session with GSS. This dataset is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This data file called "MBIS literature & GSS Expert research" excel file displays all scores derived from the GSS session held on 25 February 2012 in Veenendaal. It contains: the combined scores of all 4 experts (cross impact), the individual score from the auditor, security consultant, security officer, security architect. The experts scored based upon the Ease of Design, Ease of maintenance and Ease of Implementation of the practices. The final result is a top 20 which can function as parameter requirements in the artefact. All ranked practices (including their literature sources) are marked based upon Structure practices, Process practices and Relational Mechanism practices (SPRM). The tab BIS framework reflects the end-product, a combined score of the top 26 BISG practices categorised in Governance and executive management practices.

Group Support Session report from 25 February 2012 in PDF (167 pages). This report dataset is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design

Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This detailed report displays all the collected data during the expert panel session held on 25 February 2012 in Veenendaal. During this session a group of experts assessed Governance practices suitable for BIS that later on could function as artefact requirements.

Video footage of the expert panel (video), available on request. Not publicly available due to privacy restrictions. Available on request.

Publication on the 46th Hawaii International Conference on System Sciences (HICSS) 2013 in Hawaii United States. This publication is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. In this publication is elaborated how the research among 4 experts was done to validate the literature on Governance practices via a collaborative process and documented in GSS. The title of this publication is: Group Support Systems Research in the Field of Business Information Security; a Practitioner's View (pages 1-10) in PDF. It was presented in Hawaii in 2013 and the outcome was taken into account to further establish and demonstrate the artefact.

DOI 10.1109/HICSS.2013.244

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 6 IN APPENDIX DOCUMENT

Invite letter for Delphi Research participation in PDF

Functional Design of the MBIS artefact, core MBIS interventions

Example of the Artefact Roadmap of requirements

Artefact functional design in UML Use cases

Screenshots of youtrack artefact maintenance and backlog tool

IN DIGITAL ARCHIVE:

Excel file with Delphi research data. This data set is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. The data in this file reflects a Delphi research that was executed via a survey questionnaire in multiple rounds. The first tab represent the demographics of the participants (names and e-mails are left out). The second tab represents the answers the participants gave on Strategic forces questions and the tab "all questions" reflect all the answers the participants made. The last tab represents the summary of the strategic forces the participants are coping with during the establishment of their security plans.

Delphi research data in PDF. This data set is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. In these three PDF documents the data of the above-mentioned Delphi research is collected. It displays; demographics of the participants (42), background, role and education, The industry they are in, the BIS forces they experience (recognition of forces expressed in %), their impact, specific knowledge items the participants find vital for their industry, SMART security metrics on management and Operations.

- Report on Delphi Research part 1 in PDF (1-26 pages) reports the important strategic forces the participants experience during their strategic planning
- Report on Delphi Research part 2 in PDF (1-8 pages) reports the important arguments how organisations think they can continuous improve on BIS.
- Report on Delphi Research part 3 in PDF (1-9 pages) reports important metrics on how organisations can measure and monitor their BIS improvement efforts on a Governance, Management and Operational level. It also reports on new insights the participants gained during the filling in of the questionnaire.

Publication on Governance Practices and Critical Success factors suitable for Business Information Security at the International Conference on Computational Intelligence and Communication Networks in 2015 in PDF (1-8 pages). This paper is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This paper describes the research process of collecting literature data on BISG and validates this via the GSS expert panel to establish a core set of BIS practices and Critical Success Factors. This research was conducted in 2011 and 2012. The derived BISG practices are used in the further establishment of the BIS artefact.

DOI 10.1109/CICN.2015.216.

Publication on Porters' Elements for a Business Information Security Strategy in Information Systems Audit and Control Association (ISACA) Journal volume 1 2015. This publication reflects the research effort into strategic forces organisations cope with while drafting their strategic BIS plans.

GSS session report in PDF. This report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report displays the GSS session held on 12 April 2012 in Veenendaal among CIO's and CISO's of mid-market organisations. During this session the participants were asked to raise important management information and BIS dashboard items that can function as artefact requirements

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 7 IN THE APPENDIX DOCUMENT

Visual of the research program for establishing the artefact. This visual display the entire research program for establishing the artefact based upon several research projects.
Online tracking tool for the backlog and development of artefact requirements. Screenshot of the software development tracking tool used by the researcher and the developer
Screenshot to demonstrate the portal for online access to the artefact
ISO15504 in detail and some examples (screenshots) on how this is implemented in the artefact

Demonstration via screenshots of the BIS maturity assessment in the artefact

Screenshots to demonstrate the Software development tracker "YouTrack". This software development tracking software was used to raise new functionalities to the developer and track the development, implementation and documentation of the functionality requests.

Examples of Evidence of the taken assessments with the artefact, for benchmark purposes

Screenshots of the evaluations on the artefact
Evaluation and feedback register in Excel. This list was maintained to collect all the feedback raised during the development of the artefact.

IN DIGITAL ARCHIVE

Evaluation and Advisory report on artefact functions. This thesis report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This thesis is a contribution to evaluate and assess the core functionalities of the artefact and do a deeper analysis on the efficiency and effectivity of these functionalities in solving stakeholder problems and customer satisfaction. This research part was done in collaboration with The Hague University of Applied Sciences (Haagse Hogeschool) department Security Management, executed in 2014 and is in Dutch, page 1-95, in PDF by ST.

Thesis on the establishment and evaluation of the prototype artefact. This thesis report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report reflects the establishment of the artefact prototype and an evaluation at four organisations on multiple topics such as completeness, applicability, understandability, reliability, the goal and suggested improvements. This research part was done in collaboration with Utrecht University of Applied Sciences (Hogeschool Utrecht) department Informatics, executed in 2011 and is in Dutch, page 1-39, in PDF by SP

Adviesrapport IRO versus ISMS. This thesis report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This thesis is a contribution to compare the artefact function; Information Risk Overview (IRO) to the functionalities of an Information Security Management System (ISMS). This research part was done in collaboration with The Hague University of Applied Sciences (Haagse Hogeschool) department Security Management, executed in 2015 and is in Dutch, page 1-14, in PDF format by TA.

Group Support System on Porter and BISG research report. This summary report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report reflects a GSS session among 28 CIO's, CISO's, It managers on the topic "Cyber Security in the Boardroom" and provides insight into knowledge questions. It was held at Erasmus University in Rotterdam at 10 September 2015 (page 1-15).

Overview of the comparison criteria and video scripts. This excel report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. In this excel sheet you can find all the comparison criteria that were distilled via the ENISA based criteria, plus criteria that were distilled from this research, via an expert panel analysis and prioritisation. In this overview the top 31 criteria items with 6 votes or more in favour out of an expert panel group of 7 experts. These final 31 items were given to a two persons who demonstrated the presence of the criteria in the two MBIS artefacts (tools) via a predefined script (drafted by the person presenting the tool), and where videotaped for later validation by another expert panel group. Columns: A represents the number of the criteria, B the description of the criteria, C the score from the experts, D the script of the MBIS artefact SecuriMeter and F the script for the ISF accelerator. The videos where later on used to compare the two artefacts and do a detailed validation per criteria.

Report on the online test (step 1a). This report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report reflects the results of the test participants in round 1a of the comparison study. This comparison was executed on both tools (artefacts). In this round the test panel tested the interface, questioning, usability etc. before the next step (1b) can be executed. This test was executed online in June 2017. 14 pages in PDF named "First GSS comparison criteria".

GSS Meeting report on (step 1b blind) internet submissions on scoring the criteria on their relevance. This report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report reflects the first round of the GSS session (1b). The data in this report was collected due to pre submission of the scoring prior to the GSS sessions of 6 July 2017. Since this was submitted prior to the session the participants were not able to discuss or influence each other (blind submission). This was used as input for the physical meeting session held on the 6th July 2017 with the same participants. Page 1-16 in PDF named "Internet Session"

Meeting report on GSS session 6th July 2017 (step 1b in group) This report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report reflects the final step in

step 1 and captures the data of the GSS meeting held on 6th July 2017 with the objective to derive the core comparison criteria to in a later stage compare two artefacts on. Page 1-24 in PDF named "GSS The Hague".

SecuriMeter videopresentation (step 2). This video presentation is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This video reflects a presentation of all the predefined 37 comparison criteria (step 2) in the SecuriMeter artefact. This video is available with consent of the presenter.

ISF Accelerator videopresentation (step 2). This video presentation is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This video reflects a presentation of all the predefined 37 comparison criteria (step 2) in the ISF Accelerator artefact. This video is available with consent of the presenter.

Meeting report on GSS Session 10th August 2017 (step 3). This report is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This report contains the data capturing of the expert panel judgements during the session on 10th August 2017. This record contains the data of: Names of participants, the agenda of the session, the scores of the experts' judgment on the ISF Accelerator security tool including some comments. The scores of the experts' judgement on the SecuriMeter security tool including some comments. The opinions of experts on the question "which artefact requirements can be considered on the level of Governance, management and operations" and the opinions of experts on the process of this comparison study. It is presented in text and graphs in PDF format (page 1-22) and named "Expert Panel session of 10th August 2017"

GSS report on Session 3 in Excel. This record is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. This record contains the data capturing of the expert panel judgements during the session on 10th August 2017. This record contains the data of:

1st tab: A brief explanation on the several rounds during this comparison study. The required way of scoring via the ISO15504 methodology.

2nd and 2rd tab: The scores of the experts' judgment on the ISF Accelerator security tool including some comments. The variability between the experts judgements.

4th and 5th tab: The scores of the experts' judgement on the SecuriMeter security tool including some comments. The variability between the experts judgements

6th tab: The opinions of experts on the question "which artefact requirements can be considered on the level of Governance, management and operations"

7th tab: The opinions of experts on the process of this comparison study

8th tab: Names of participants (blanked out in the public version)

9th tab: Final mapping of the criterias and the comparison between the two artefacts

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

APPENDICES THAT ACCOMPANY CHAPTER 8

Screenshot of the BIWA. This screenshot is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. These screenshots reflect the various assessments variants that are built in the artefact for measuring the security levels within; water companies that need to comply to the BIWA (Baseline Informatiebeveiliging Waterschappen). It also includes a screenshot of the BIWA dashboard and the BIWA benchmark in the water company industry.

Screenshot of the implementation of the ITOMM. This screenshot is a contribution to the PhD thesis research effort "On a collaborative analysis method for Improving the Maturity of Business Information Security (MBIS). In this research a Design Science research Artefact was established to measure, monitor and report how organisations can improve their Business Information Security levels. These screenshots reflect the IT Objective Maturity Model (ITOMM) build in the artefact for measuring the security levels based upon the ITOMM model. Screenshot on the implementation of the ITOMM measurement scales, questions, graphs, dashboard etc. Mainly used for future development of the ITOMM model.

Notification letter of the European Security Breach / incident notification act July 2012 in PDF. In this act specific vital industry companies are subject to a new notification act to notify if they are victim of a significant data breach or incident.

The appendices are accessible via the Radboud University digital archive, structured per chapter. Accessed via <http://dx.doi.org/10.17026/dans-zbu-hfdc>

THE ENTERPRISE ENGINEERING NETWORK

BACKGROUND

The Enterprise Engineering Network (EE Network, www.ee-network.eu) is a research and training network targeting PhD candidates and research fellows. Next to the supervision of PhD candidates and research fellows, the main activities of the network involve:

- Research seminars;
- Events targeting interaction with practitioners;
- Events targeting interaction with M.Sc. students;
- Development of a joint curriculum for EE Network researchers and associated courses;
- Co-organisation of scientific events.

The hosts of the network are also concerned with formulating and conducting joint research projects. Yet, the EE Network itself focuses on the actual training activities. The history of the EE Network, and its direct predecessors, can be traced back to 2001. It is currently hosted at six locations:

1. Headquarters: IT for Innovation Services department of the Luxembourg Institute of Science and Technology, Belval, Luxembourg;
2. Université de Lorraine, Nancy, France;
3. University of Luxembourg, Luxembourg, Luxembourg;
4. Radboud University, Nijmegen, the Netherlands;
5. HAN University of Applied Science, Arnhem, the Netherlands;
6. Utrecht University of Applied Science, Utrecht, the Netherlands.

To enable a practical operation of the training activities, in particular for the research seminars, the EE Network has a traditional geographical focus on the Rhine-Scheldt-Meuse-Moselle basin, which includes the Low Countries (Belgium, Netherlands and Luxembourg), the Rhineland in Germany, as well as Lorraine in France.

FINISHED DISSERTATIONS

Dissertations produced in the EE Network, and its direct predecessors, include:

2018-1 M. Bjeković, Pragmatics of Enterprise Modelling Languages: A Framework for Understanding and Explaining, Radboud University, Nijmegen, the Netherlands, January 12, 2017

2017-2 M. van Zee, A recommender system to support high-level decision making in large companies Rational architecture: Reasoning about enterprise dynamics, University of Luxembourg, Luxembourg, April 6, 2017

2017-1 G. Plataniotis, EA Anamnesis A Conceptual Framework for Enterprise Architecture Rationalization, Radboud University, Nijmegen, the Netherlands, April 4, 2017

2016-2 R. Ettema, Using triangulation in Lean Six Sigma to explain quality problems - An enterprise engineering perspective, Radboud University, Nijmegen, the Netherlands, December 14, 2016

2016-1 H. Faller, Organizational Subcultures and Enterprise Architecture Effectiveness: an Ex-planatory Theory, Radboud University Nijmegen, Nijmegen, the Netherlands, March 4, 2016

2015-2 L.J. Pruijt, Instruments to Evaluate and Improve IT Architecture Work, University of Utrecht, Utrecht, the Netherlands, November 25, 2015.

2015-1 D.J.T. van der Linden, Personal semantics of meta/concepts in conceptual modeling languages, Radboud University Nijmegen, Nijmegen, the Netherlands, February 13, 2015.

2014-2 C. Feltus, Aligning Access Rights to Governance Needs with the Responsibility MetaModel (ReMMo) in the Frame of Enterprise Architecture,

University of Namur, Namur, Belgium, March 11, 2014.

2014-1 F. Tulinayo, Combining System Dynamics with a Domain Modeling Method, Radboud University Nijmegen, Nijmegen, the Netherlands, January 27, 2014.

2013-2 C. Brandt, An Enterprise Modeling Framework for Banks using Algebraic Graph Transformation, Technische Universität at Berlin, Berlin Germany, December 20, 2013.

2013-1 R. Wagter, Enterprise Coherence, Radboud University Nijmegen, Nijmegen, the Netherlands, November 19, 2013.

2012-2 A. Nakakawa, A Collaborative Process for Enterprise Architecture Creation, Radboud University Nijmegen, Nijmegen, the Netherlands, November 21, 2012.

2012-1 D. Ssebuggwawo, Analysis and Evaluation of Modelling Processes, Radboud University Nijmegen, Nijmegen, the Netherlands, November 21, 2012.
2009-2 S. Overbeek, Bridging Supply and Demand for Knowledge-Intensive Tasks, Radboud University Nijmegen, Nijmegen, the Netherlands, April 24, 2009.

2009-1 J. Nabukenya, Improving the Quality of Organizational Policy Making using Collaboration Engineering, Radboud University Nijmegen, Nijmegen, the Netherlands, March 3, 2009.

2006-1 B. van Gils, Aptness on the Web, Radboud University Nijmegen, Nijmegen, the Netherlands, March 3, 2006.

2004-1 S.J.B.A. Hoppenbrouwers, Freezing Language { Conceptualisation Processes across ICT Supported Organizations, Radboud University Nijmegen, Nijmegen, the Netherlands, December 10, 2004.

IT Security is becoming more complex and is changing more rapidly. It has implications beyond the IT field, touching all the essential aspects of companies' governance, management and operations. Since businesses increasingly rely on information and their supporting processes Information Security is more and more seen as part of Business Administration in close collaboration with key stakeholders that subsequently benefit the well-being of the firm. We therefor refer to the term "Business Information Security" (BIS). The causes of the many security incidents that take place are very diverse, as are the strategies that have been chosen to keep them manageable.

The main problem we aim to tackle in this research project is, on the one hand to contribute to the required knowledge sharing, build consensus on the priorities (where to start), create the necessary engagement among stakeholders and make informed decisions to achieve objectives. In this book we refer to the collective term "Collaboration". And on the other hand we determine key concepts that underpin Maturing Business Information Security (MBIS) and practices that support the required analytical- and administrative work without reinventing the wheel. The main question answered in this book is "How can we establish a collaborative analysis method which utilises best practices for improving the maturity of BIS?"

This study has benefited from enthusiastic co-operation from many parties and has resulted in a method that enables collaboration and administration to improve the Maturity of Business Information Security. That aligns business with information security and is tested in practical environments. The produced artefact can utilize industry best practices and has the required functionalities that contribute in the improvement of BIS.

Furthermore this research project gives insights in practices, enablers and critical success factors for BIS that organisations can incorporate in their business and encourages other academics to do further research on..

You can improve things.

You cannot mature things, since maturing happens as a natural process.

Thus we can only strive to improve the maturing process.