IMPROVING THE MATURITY OF BUSINESS INFORMATION SECURITY

Y. Bobbert

On the Design and Engineering of a Business Information Security Artefact

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 promotors 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 promotors 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 in-formation 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 prac-tices 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 could 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 organisations 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

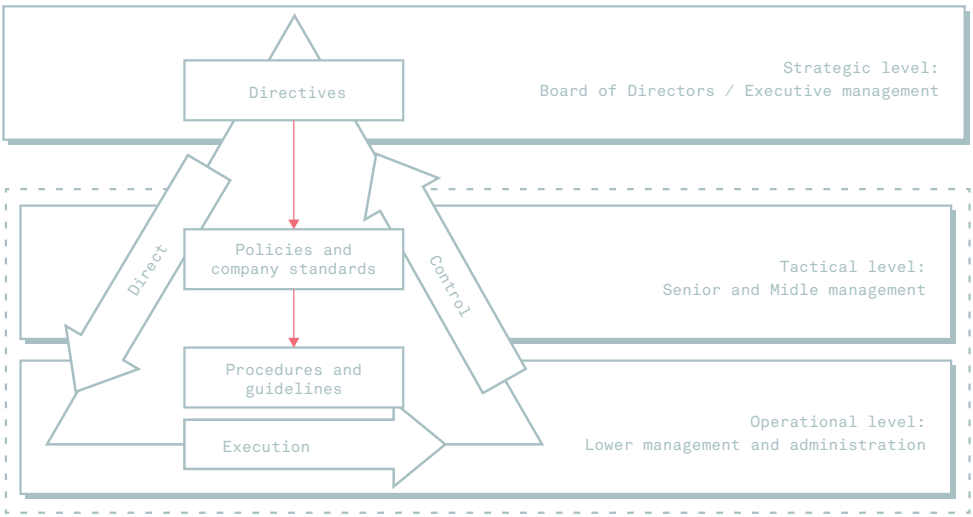

Figure 1: The IS Governance Direct Control Cycle taken from Von Solms and Von Solms [57].

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.

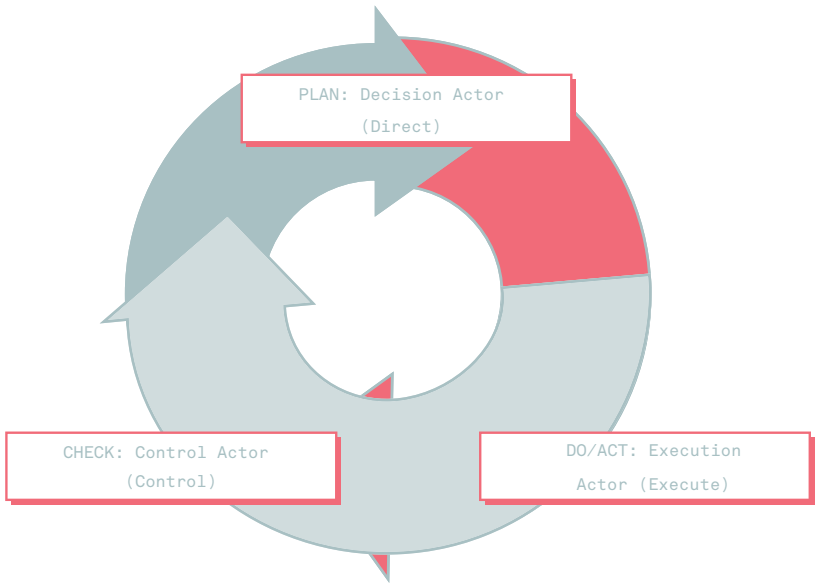

Figure 2: The PDCA cycle on Direct Control Cycle of Van Solms & Von Solms based on Tewarie [66].

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

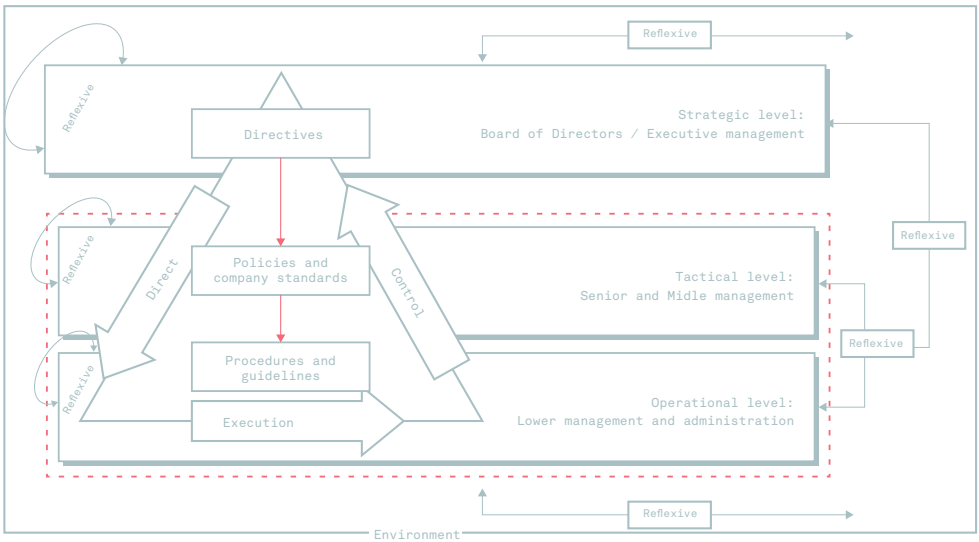

Figure 3: Conceptual Model based on the Direct Control Cycle of Von Solms and Von Solms [71].

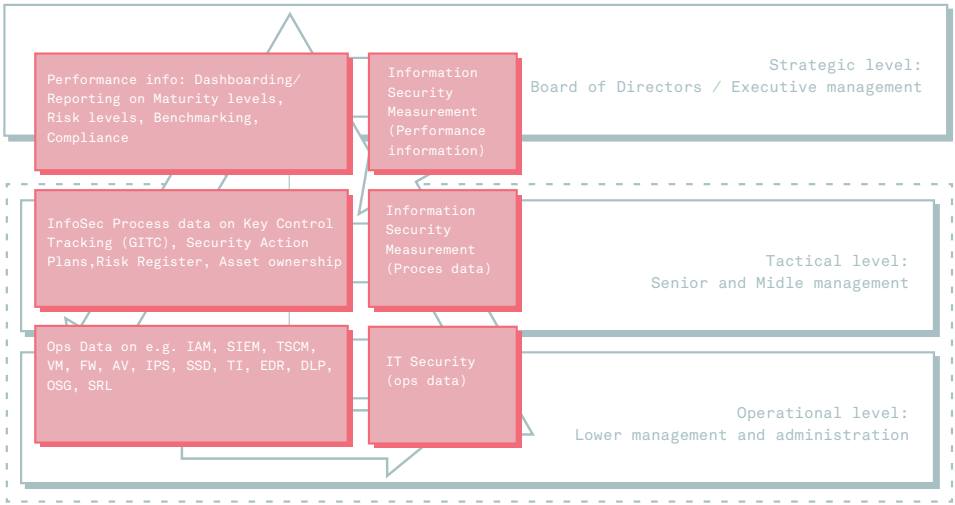

Figure 4: Conceptual model with detailed BIS processes and data, based on Von Solms and Von Solms [71].

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 Perjons [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 practical[1] 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.

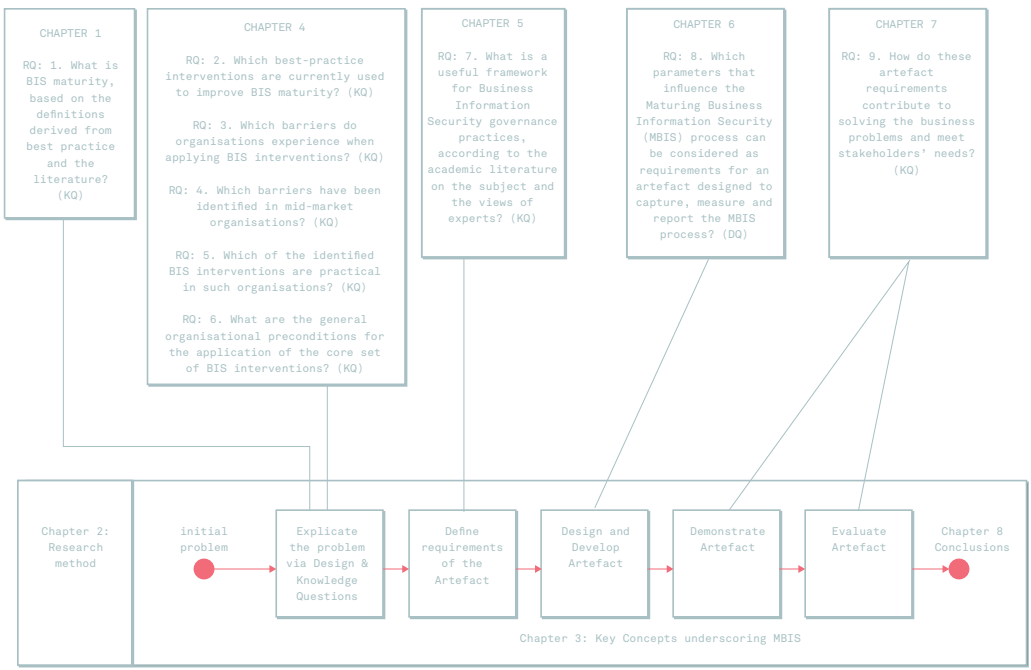

Figure 5: Thesis structure including research questions based upon Johannesson and Perjons [73]

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.

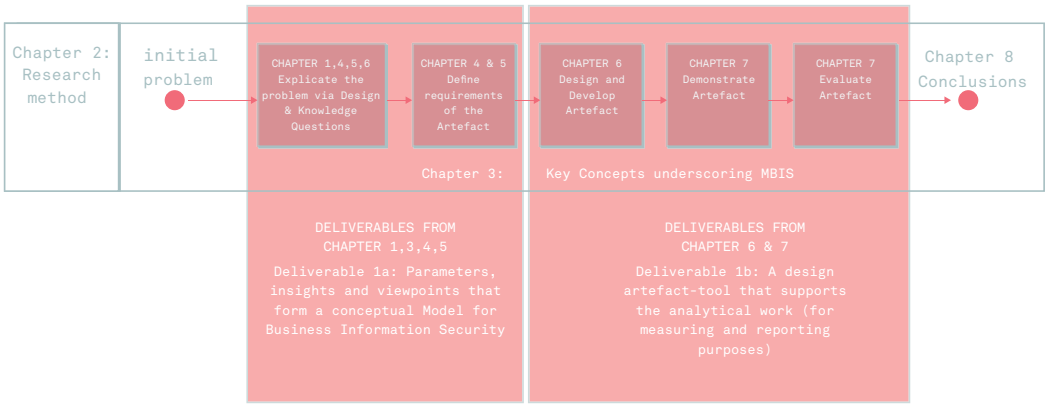

Figure 6: Thesis structure with deliverables based upon Johannesson and Perjons [66]

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.

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 therefore 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.

Dr. Yuri Bobbert MSc CISM CISA SCF is the global Chief Information Security Officer (CISO) at NN-Group N.V. and the former ad interim CISO of UWV (Government - Financial services). Prior to his role as an interim CISO he served for 10 years as CEO of a consulting firm. Bobbert is visiting professor at Antwerp University, Antwerp Management School and author of several books and publications in Business Information Security Governance and Management.

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.

9 789461 263223

DIALOG