Governance Practices and Critical Success factors suitable for Business Information Security

Yuri Bobbert
University of Antwerp
LOI University of Applied Sciences
yuri.bobbert@ua.ac.be

Hans Mulder
University of Antwerp
Antwerp Management School
hans.mulder@ua.ac.be

Abstract— Information Security (IS) is increasingly becoming an integrated business practice instead of just IT. Security breaches are a challenge to organizations. They run the risk of losing revenue, trust and reputation and in extreme cases they might even go under. IS literature emphasizes the necessity to govern Information Security at the level of the Board of Directors (BoD) and to execute (i.e. plan, build, run and monitor) it at management level. This paper describes explorative research into IS-relevant Governance and Executive management practices. Answering the main research question: "Which practices at the level of Governance are relevant for Business Information Security Maturity" The initial phase of this research consists of a review of academic and practice-oriented literature on these relevant practices. This list of practices is then examined and validated through expert panel research using a Group Support System (GSS). The paper ultimately identifies a list of 22 core principles. This list can function as frame of reference for Boards of Directors and Management Teams in order to increase their level of Business Information Security (BIS) Maturity.

Keywords—Business Information Security Governance, Corporate Governance, Information Security Management, Risk Management, Security Governance Principles

I. INTRODUCTION

The main origin of this research paper is concern about the low awareness of security issues on the part of businesses. [1] [2]. Theorists and practitioners generally observe good security management [3] practices but also indicate that less attention is paid to Governance practices [4] [5] [6]. This is a problem because security breaches have tremendous implications for the continuity [7], civil or legal liability [8], reputation [9], employability and financial position of firms [1] [10]. Hence, it could be argued that Information Security, and its implications, no longer only affects the IT department but consists of multiple disciplines (i.e. risk management, finance, auditing, marketing [11]). The term "Business Security" was introduced by Von Solms in 2005 [12] to be followed by the more comprehensive term "Business Information Security" which refers to the domain of critical information protection and security [13].

Recent research has shown that the number of security incidents has increased over the years, as has the financial impact per data breach [2]. In 2009, 25% of EU organizations experienced a data breach (with 47% of Finnish organizations in the leading position). As a result, the European economy has suffered an annual multi-billion loss in Euro's (source: Europol). The main causes of security incidents are the multiplication of data (Big Data) and social media interaction [14], and the increase in cybercrime activities [15] [16].

Research conducted in 2010 found that 39% of the examined organisations revealed an average security maturity of 2 out of 5 [17]. Empirical (measurements) research performed over 2012 and 2013 within 27 organizations confirmed that companies predominantly 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 3 years, mainly because the current frameworks are "complex and generic", as Siponen and Wilison argue [18].

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 3 domains out of 12 in the ISO27001 framework, presented in figure 1. The absence of a dedicated Security Governance Maturity Model and clear practices that can be adopted by Boards is a limitation. This research aims to remedy this problem by investigating, ordering and ranking relevant practices.

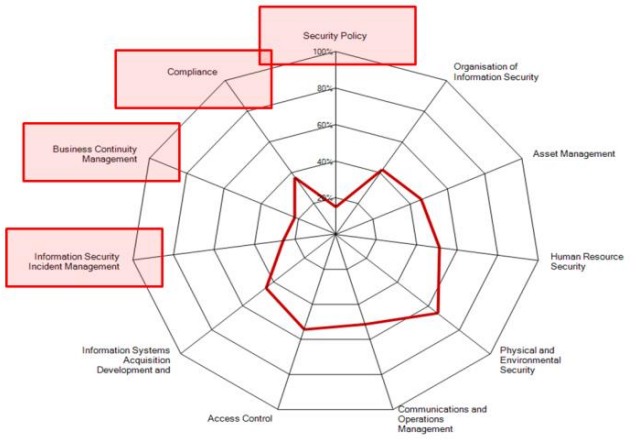

Figure 1: Information Security Maturity of 27 Dutch organizations (2012-2013)

978-1-5090-0076-0/15 $31.00 © 2015 IEEE
DOI 10.1109/CICN.2015.216

II. PROBLEM STATEMENT

This low level of security maturity and the absence of clear governance practices bring us to the problem statement of this research project, namely; A lack of insight into governance practices that can successfully function as a core set of principles that can potentially contribute to the increase of Security Governance Maturity of organizations.

It is the researchers' intention to contribute to academic rigor 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)"*. Predominantly sets the direction.

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

Even though theorists and practitioners bodies like ISACA emphasize Governance involvement in securing and assuring the critical assets, practice shows the opposite [17] (illustrated in Figure 1). To address this challenge, information security governance is increasingly becoming an academic discipline to cross this "knowing-doing-gap". Basie and Rossouw von Solms [4] define Information Security Governance (ISG) as: "ISG consists of the management commitment and leadership, organizational 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, organizations have become more successful in implementing security management but are still struggling with the implementation of information security governance [19] [20]. 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 [21]. All activities to effectuate these activities into decisions is seen as management and thus beyond the scope of this literature review. This is also valid for operational practices.

In this paper we follow Van Solms' distinction between Governance and management [20] [21]. Furthermore, we specifically distinguish between Executive management activities and Senior and Middle management activities (Figure 2). For semantics we use the collective term Governance (where we also mean Executive management).

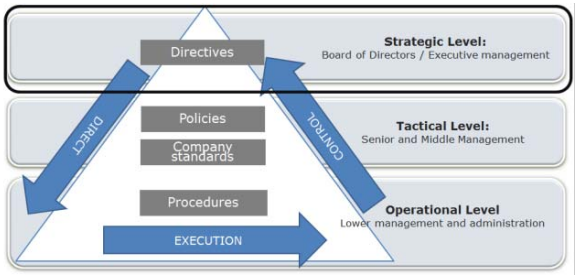

Figure 2 The Corporate Governance Direct–Control Cycle (Von Solms 2006).

III. DEFINING THE RESEARCH QUESTION

The main research question (MRQ) underlying this research project is as follows:

MRQ *"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 is proposed (academic as well as practitioner- oriented literature).

Numerous IT Governance studies [22] [23] [24] [25] propose process-oriented practices, structure-oriented practices and culturally oriented practices to effectuate 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 emphasize 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 [23] [26] 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 rigor 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 multiple perspectives?*

IV. Research Methodology & Approach

A. Literature research

Research in the field of Governance for Information Security is rare. Such work as exists is based on practitioners [27] [2] [3]. 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 is aimed at exhaustively investigating relevant literature over multiple years (2009-2012) and listing them in a structured way using the methodology proposed by Bruce in 1994 [28]. Other disciplines closely related to BISG were investigated. Being, Corporate Governance (CG), Risk Governance (RG), Information Security Governance (ISG) and Information Technology Governance (ITG).

B. Structures, Processes and Relational Mechanisms

As mentioned before, earlier research by Van Grembergen & De Haes [29] and Luftman [30] served as a starting point for aligning business goals to governance practices [29]. De Haes & Van Grembergen [31] [32] suggest deploying a collective set of structures, processes and relational mechanisms (e.g. culture, knowledge) in order to successfully effectuate IT governance in organizations. In this research we propose the same methodology to mark the literature data, and subsequently distill a core set of practices and CSF's that can be used by practitioners. As described, this theory was successfully applied in previous studies [29] and led to effective and practical methods [13] [33].

C. Rigor & Relevance

Most of the current rigor in the Security domain is prescriptive in nature. To acquire a more profound understanding of the gap between what needs to be done according to rigor and what is prioritized by practitioners (relevance) a validation by practitioners of the collected list is required. Firstly, we need to know which practices are absent from the literature and might cause this 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 on multiple perspectives (relevance criteria i.e. effect, ease of design, implementation, and maintaining) and rank them in order to achieve a certain sequence in the application of the practices. Figure 3 displays the research process flow in order to find answers to the research questions.

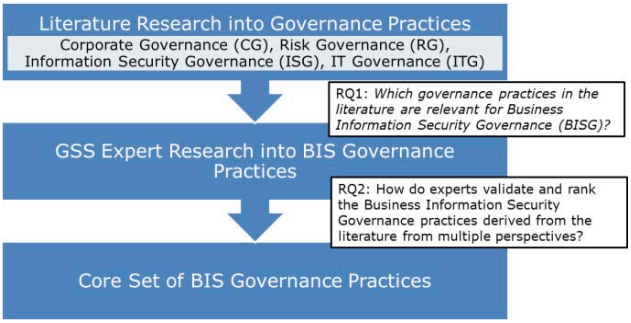

Figure 3 Research Process including Research Questions

D. GSS Expert Research

After the collection of all the literature data, expert views are 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 [34] [35]. 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 [36].

Moreover, the number of items (in this case 228 practices) to be discussed is an important variable in the set-up 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 [37]. The experts were selected according to the following criteria: they have a BA or MA degree in Information Systems, completed with industry certificates e.g. Certified Information Security Manager (CISM), Chief Information Security Auditor (CISA), Certified Ethical Hacker (CEH), Register EDP-auditor (RE). They have more than 10 years of experience in Business Information Security and they are full-time practitioners in Business Information Security. The 4 experts are perfectly situated to select and rank this huge amount of literature data which makes their assessments highly relevant.

V. Research Findings

A. Literature Review

Literature predominantly refers to Governance where it actually appoints executive management practices (e.g. C-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 [4], are;

1. Corporate Governance,
2. Risk Governance,
3. Enterprise Governance of IT and
4. Information Security Governance

1. Approximately 50 best practices from the **Corporate Governance** discipline were examined. Major sources of origin of these practice are: The OECD Principles of Corporate Governance [38]. The Commonwealth Association for Corporate Governance [39]. Internal Control Guidance to Directors, Turnbull report [40], The Financial Reporting Council (FRC) Combined Code [41]. The King Report on Corporate Governance for South Africa [42]. Bank for International Settlements (BIS) Basel principles for enhancing corporate Governance [43]. Security and Exchange Commission add-ons to SoX, Commission on Public Trust and Private Enterprise 2003. All of them can be found in the Corporate Governance Book (Oxford University Press) which covers all international Corporate Governance codes [44].

2. A major component of practicing good Governance is the **Risk Governance** discipline. Insufficient Risk Governance and management have enormous consequences for all major stakeholders [45]. The judgment and management of IT-related risks has become increasingly important to the success of businesses [46]. For the assessment of all relevant Risk Governance practices, the researcher examined literature from: COSO's Enterprise Risk Management Integrated Framework [47], COSO's "Embracing Enterprise Risk Management": Practical Approaches for Getting Started [48], COSO's "Where Board of Directors currently Stand in executing Their Risk Oversight Responsibilities" [49], King's Report on Corporate Governance for South Africa – 2002 [42], 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?" [11], 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" [25] and De Haes & Van Grembergen's study "Implementing Information Technology Governance; Models Practices and Cases" [31] and Van Grembergen's "Strategies for Information Technology Governance" [32].

During the selection of the literature, numerous academic and practice-oriented sources were investigated, predominantly to judge their appropriateness for ISG practices. The researcher investigated a large number of resources on **Information Security Governance,** because this discipline is the most closely related to (BISG). The researcher 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). The researcher also looked at best practices institutes such as ISACA, ITGI, ISF, SABSA etc., and other communities practicing 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 [50] 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 [51]. Von Solms' "The 10 deadly sins of information security management" [51] and other major relevant sources on the ISG topic [52] [53] [54] [55] [56] [57] [4].

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 operationalized. This was done by the experts..

B. Discussion & 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 recognize 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 [42] and The United States [50]. These countries specifically address technology risks in their practices, predominantly because they suffer the most from cyber criminality. At the time of writing, the European commission also addressed Cyber Risks as a "Board responsibility".

The researcher has observed the usability of a tremendous amount of Corporate and Risk Governance practices applicable in the domain of BIS. Judging from practical experience, basic principles such as; determine responsibility and accountability (Turnbull Report, COSO, King Report) and the role of the Stakeholder [39] [49] are not effectuated by organizations.

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

C. GSS Expert Research

The initial list of 228 practices was further evaluated by a group of four experts during a 4 hour GSS session led by an

experienced facilitator. In the first round of this evaluation, the experts were asked to justify the quality (adding, un-doubling) of the practices. This took 2 hour all experts in one group each 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 & realization, ease of maintenance and ease of implementation. This took 3 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 organization does not know how. Because of this vague specification of important Governance Practices, the researcher asked the experts to rephrase them into a more understandable format. Many of the Corporate Governance practices are a derivative 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 organization.

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 the researcher that the 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 organization but it is less fully integrated than for example risk management (risks arise on multi-levels, 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 organizing the Information Security Governance Practices.

The final item on the agenda of the expert panel session was the organization 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 is having the experts assess all of them and make comments if they disagree.

An important consideration for the researcher 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 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 literature data. 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 is used in the next "ranking" phase.

D. Ranking the Governance practices

After the expert panel had compiled a set of practices, it was important to rank them on relevance for an organization. In order to compile a comprehensive and practical list that can function as principles, the researcher formulated these four ranking criteria as 1. Effectiveness, 2. Ease of Design and Realization, 3. Ease of maintenance and 4. Ease of Implementation. The result should be a frame of reference of core principles.

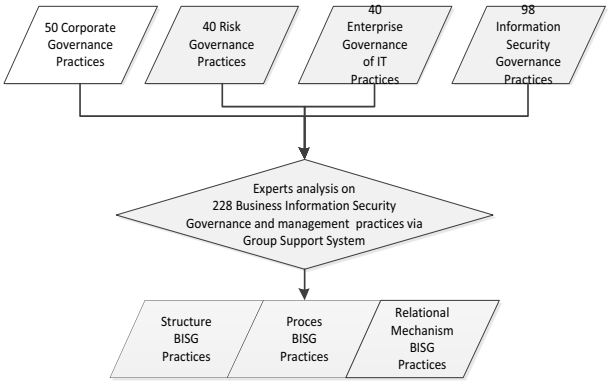

Figure 4 Conceptual Model of the Literature Research into relevant disciplines

The level of effectiveness is 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 can later be used as candidates for the next selection "Ease of Design and Realization", Ease of maintenance and Ease of implementation, also from 0-5. Assessing and ranking all practices over these three dimensions will enable the researcher to comprehensively select the practices which can be monitored and evaluated by the Board (Governance level). In consensus with the experts the researcher decided to rank the top practices, measured from 4 and above on effectiveness. Consensus was achieved due to all experts voting in favor to limit the amount 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 cumulated score of the sum of the score per criterion.

VI. DISCUSSION, LIMITATIONS & CONCLUSIONS

We can conclude that experts consider the current literature on practices to be rather vague and complex. They supported

that 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 [58]. Empirical research within 27 organisations also demonstrates this consequence. Some literature suggests more simple and practically oriented practices - *Report simple (Red-Yellow-Green) & Do simple risk assessments* - with the intention to increase 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 effectuate 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 due to the score of 2.5.

Our final finding is that the top practices needed to be undoubled 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 rigor 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 (table I & II). This list can function as reference for Boards of Directors and Management teams to effectuate the Governance process of Direct-Control. By making a clear distinction between Governance and Executive management, the practices are applicable in various organizations (independent of a one-tier board or two-tier board).

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, the researcher and the experts compiled a final list of BISG practices that can function as a frame of reference for Board of Directors. Moreover, this list of "principles" may serve as basic parameters of the level of BISG maturity within organisations. Thus, before organisations are able to mature on 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 principles and the proposed method, to enhance the BISG Maturity of organisations. Future research will try and capture maturity levels of BISG by incorporating the method described in this article into an artifact coined as "Securimeter" with the objective to capture valid data on best practices that are relevant for further scientific research. And further enhance the BISG maturity within organisations.

TABLE I. TOP 20 GOVERNANCE PRACTICES AND CRITICAL SUCCESS FACTORS FOR BUSINESS INFORMATION SECURITY

Rank	Score	Practice
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 KPI's
20.00	8.00	Alignment strategy and approvement by board.

TABLE II. TOP 10 GOVERNANCE PRACTICES AND CRITICAL SUCCESS FACTORS FOR BUSINESS INFORMATION SECURITY 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. kind 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 a 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 program's adequacy and effectiveness.	10.00	Management	Process
10	**Ensuring the integrity of the corporation. A**ccounting and financial reporting systems. including the independent audit. 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

REFERENCES

[1] M. Ishiguro. T. Hideyuki. K. Matsuura and I. Murase. "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market." The Graduate School of Interdisciplinary Information Studies. The University of Tokyo. p. 15. 2011.

[2] Ponemon Institute. "Business Case for Data Protection." Ponemon Institute LLC. 2009.

[3] AberdeenGroup. "Best Practices in Security; Governance." Aberdeen Group. Inc. Boston. Massachusetts. 2005.

[4] S. von Solms and R. von Solms. Information Security Governance. New York: Springer Science (ISBN 978 0 387 79983 4). 2009.

[5] 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].

[6] ITGI. "Information Security Governance. Guidance for Boards of Directors and Executive management 2nd edition." IT Governance Institute . United States. 2006.

[7] R. Prins. "Diginotar Bancruptcy Public Report." Dutch Government. Den Haag. 2011.

[8] A. C. Johnston and R. Hale. "Improved Security Through Information Security Governance." Communications of the ACM. vol. 52. no. 1. pp. 126-129. 2009.

[9] F. Peters. Reputatie onder druk; Het managen van reputaties in een veranderende samenleving. Den Haag: SDU Uitgevers. 2012.

[10] 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.

[11] ITGI. "Information Risks; Who's Business are they?." IT Governance Institute. United States. 2005.

[12] V. Solms. "From Information Security to business security." Computer & Security. Elsevier. South Africa. 2005.

[13] Y. Bobbert. Maturing Business Information Security. A Framework to establish the desired state of Security Maturity. Utrecht: IBISA. 2010.

[14] C. Everett. "Social Media; Opportunity or risk." Computer Fraud Security. 2010.

[15] Y. Jewkes and M. Yar. Handbook of Internet Crime. UK: Willan Publishing. 2010.

[16] W. Fan and K. Yeung. "Online Social Networks - Paradise of Computer viruses." Science Direct. University of Hong Kong. 2011.

[17] 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.

[18] M. Siponen and R. Willison. "Information Security management standards: problems and solutions." Information & Management 46. Finland. 2009.

[19] B. Solms. "Corporate Governance and Information Security." Computers and Security. 20 215-218. South Africa. 2001.

[20] B. v. Solms and S. Posthumus. "A framework for the governance of information security." Elsevier Ltd. South Africa. 2004.

[21] R. Solms von and B. Solms von. "Information Security Governance_ A model based on the Direct–Control Cycle." Computers and Security. vol. 25. no. Science Direct. pp. 408-412. 2006.

[22] S. De Haes and W. Van Grembergen. "Practices in IT Governance and Business/IT Alignment." Information System Control Journal. Volume 2. 2008.

[23] R. Peterson. "Integration Strategies adn Tactics form Information Technology Governance." in Strategies for Information Technology Governance. Idea Group Publishing.. 2003. pp. 37-80.

[24] W. Van Grembergen. "Structures. Processes and Relational Mechnisms for IT Governance." in Strategies for Information Technology Governance. US. Idea Group Publishing.. 2004. pp. 1-36.

[25] P. Weill and J. Ross. IT Governance. Boston Massachusetts: Harvard Business School Press. 2004.

[26] B. De Wit and R. Meyer. Strategy Synthesis: Resolving Strategy Paradoxes to Create Competitive Advantage 2nd ed. London: Thomson . 2005.

[27] Forrester. "The Forrerster Wave: Information Security and risk consulting services." Forrerster Research . USA. 2010.

[28] C. Bruce. Research Students: Early Experiences of the dissertation literature review. Studies in Higher Education. 1994.

[29] S. De Haes and W. Van Grembergen. "Enterprise governance of IT. Achieving strategic alignment and value." Springer. New York. 2009.

[30] J. Luftman. "Assessing Business-IT Alignment Maturity." Communications of the Association for Information Systems. vol 4. art 14. US. 2000.

[31] W. Van Grembergen and S. De Haes. Implementing Information Technology Governance; Models Practices and Cases. Hershey. United States: IGI Publishing. 2008.

[32] W. v. Grembergen. Strategies for Information Technology Governance. United States: Idea Group Publishing. 2004.

[33] ISACA. Cobit5: for Information Security. ISACA. 2012.

[34] 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.

[35] R. Newby. G. Soutbar and J. Watson. "Group Support System Approach." International Small Business Journal. vol. 21. no. 4. pp. 421-433. 2003.

[36] 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.

[37] A. Rutkowski. B. Van de Walle and G. van den 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.

[38] OECD. "The OECD Principles of Corporate Governance." ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Paris. France. 2004.

[39] CACG. "CACG GUIDELINES PRINCIPLES FOR CORPORATE GOVERNANCE IN THE COMMONWEALTH Towards global competitiveness and economic accountability." Commonwealth Association. Marlborough. New Zealand. 1999.

[40] FRC. "Revised Turnbull Guidance." Financial Reporting Council. UK. 2005.

[41] FRC. "THE UK CORPORATE GOVERNANCE CODE." FINANCIAL REPORTING COUNCIL. UK. 2010.

[42] King. "King report on Corporate Governance for South Africa." King Committee on Corporate Governance. SA. 2002.

[43] BIS. "Principles for enhancing corporate governance." Bank for International Settlements 2010.. Basel Switzerland. 2010.

[44] C. Mallin. Corprate Governance. Third Edition. New York: Oxford University Press. 2010.

[45] D. Hubbard. The Failure of Risk Management. Hoboken New Jersey: John Wiley & Sons. 2009.

[46] G. Westerman and R. Hunter. IT Risk. Turning Business Threats into Competitive Advantage. Boston MA: Hardvard Business School Press. 2007.

[47] COSO. "Enterprise Risk Management Integrated Framework." September 2004. [Online]. Available: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf. [Accessed 22 10 2010].

[48] COSO. "Embracing ERM. Practical Approaches for Getting Started." Committee of Sponsoring Organizations of the Treadway Commission. United States. 2011.

[49] COSO. "Where Board of Directors currently Stand in executing Their Risk Oversight Responsibilities." COSO. United States. 2011.

[50] CGTF. "The Corporate Governance Task Force Report. Information Security Governance: A CALL TO ACTION.." National Cyber Security Summit. United States. 2004.

[51] S. De Haes and W. Van Grembergen. "Practices in IT Governance and Business/IT Alignment." Information System Control Journal. Volume 2. 2008.

[52] H. Kruger and W. Kearney. "A prototype for assessing information security awareness." Science Direct; Computers & Security 25 (289-296). South Africa. 2006.

[53] S. El Aoufi. "Economic Evaluation of Information Security." Vrije University Press. Amsterdam. 2009.

[54] M. Frigo and R. Anderson. "Embracing Enterprise Risk Management: Practical Approaches for Getting Started." 2011. [Online]. Available: http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_001.pdf. [Accessed 22 October 2011].

[55] 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.

[56] F. Conner and A. Coviello. "Information Security Governance: A call to action." The Corporate Governance Task Force. United States. 2004.

[57] ISACA. "An Introduction to the Business Model for Information Security." ISACA. United States. 2009.

[58] Kluge et al. "Formal Information Security Standards in German Medium Enterprises." in Conisar. Phoenix. 2008.

[59] Golden-Biddle. Composing Qualitative Research. Thousand Oaks: SAGE. Eason. B. Noble. and I.N. Sneddon. "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions." Phil. Trans. Roy. Soc. London. vol. A247. pp. 529-551. April 1955.