Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations

Edward Bernroider, Sebastian Margiol, Alfred Taudes

Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations

Edward W. N. Bernroider, Sebastian Margiol (✉), Alfred Taudes

Institute for Information Management and Control
Vienna University of Economics and Business, Welthandelsplatz 1, 1020 Vienna, Austria
{edward.bernroider, sebastian.margiol, alfred.taudes}@wu.ac.at

Abstract. This paper describes the development of an information security framework that aims to comparatively assess the quality of management processes in the context of cyber-security of organizations operating within critical infrastructure sectors. A design science approach was applied to establish a framework artifact that consists of the four dimensions “Security Ambition”, “Security Process”, “Resilience” and “Business Value”. These dimensions were related to the balanced scorecard concept and information security literature. The framework includes metrics, measurement approaches and aggregation methods. In its adapted form, our framework enables a systematic compilation of information security, and seeks to display the security situation of a focal firm against the desired future states, industry benchmarks, and allows for an investigation of interdependencies. The design science research process included workshops, cyclic refinements of the instrument, pretests and the framework evaluation within 30 critical infrastructure organizations. The framework was found to be particularly useful as learning and benchmarking tool capable of highlighting weaknesses, strengths, and gaps in relation to standards.

Keywords: BSC · Cyber-security · Critical Infrastructure · Design Science · Information Security Management

1 Introduction

Today's organizations in the private and public sectors have become increasingly dependent on Information and Communication Technologies (ICTs) to develop and offer their services and products. While these ICTs offer considerable advantages, their widespread access expose individuals, organizations and nations to risks, which in particular include Internet-related security breaches [1]. A missing understanding of the risk cultures and exposures related to developing and operating ICT can lead to significant negative impacts. Consequently, there is a natural interest of a wide range of stakeholders including citizens and governments [2] to ensure that any organization in an economy, in particular those operating critical infrastructures, manage their ICT risks ap-

adfa, p. 1, 2011.

propriately. An infrastructure is considered to be critical when its maintenance is essential for vital societal functions. A damage to a critical infrastructure, such as energy supply or transportation [3], may have a significant negative impact for the security of the country and the well-being of its citizens.

An important and growing area of research and standard development deals with organizational-related cyber-security issues. Cyber-security has been defined by the International Communications Union (ITU) to mean "a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user's assets" [4]. The term can be considered to holistically cover all ICT related threats, e.g., involve corrupting or disrupting e-services or simply the information flow between people and organizations. Organizational and user assets include all resources (information, people, technologies and systems).

When characterizing cyber-security studies, one needs to understand what is measured, why and for whom the measurement takes place [5]. In our case, we seek to measure critical infrastructure organizations, which are of particular importance to the stability of a nation or economy [2]. The motivation is to allow for a description and comparison of cyber-security in terms of overall performance of information security management (ISM) and its strategic security programs, which are the foundation for achieving security on the technical infrastructure level. While technical scores are important to understand the many facets of operational security including the configuration of firewalls, the effectiveness of intrusions detection systems [6] or the use of proxy servers, strategic scores allow for an understanding of how well risks are being predicted or managed, whether policy compliance is reached or business impact analysis is sufficient enough. Finally, we seek to feedback information to the critical infrastructure organizations and to serve external authorities and policy makers, who can support cyber-security with a range of tools, e.g., research and development programs.

An important element of cyber-security is to protect an entity based on given security objectives against risks in the cyber-environment. Multi-dimensional framework approaches can be used to assess and control levels of performance [7], in particular in relation to cyber-security [8]. The strategic and measurement focus of this study made us consider balanced scorecards (BSCs) approaches, which offer a systematic analysis linking strategy with a set of measures [9-11]. Such scorecards typically display the current security situation against the desired future states in an attempt to systematically manage cyber-security of an organization, which is also unit of analysis for this study.

The aim of this paper is to build and test a framework that can be used to holistically measure the quality of information security management in the context of cyber-security and allow for comparative assessments of organizations in critical infrastructure sectors. This context requires to generally include the management of ICT security in organizations with a focus on the strategic level holistically covering an entire organization. We were also interested in the typical frameworks and their metrics, measurement approaches and aggregation methods to operate a scorecard. This scorecard should consider the requirements to be able to evaluate and compare a given security-level, and had to be implementable by face-to-face interview techniques implemented as part of a survey. The following section gives a preliminary theoretical overview based on academic literature and standards to identify relevant prior research focused on scorecards and their constituent elements. A design science approach is used to develop an assessment framework as an artifact based on scorecard theory and fieldwork including workshops and empirical validations.

2 Theoretical Background

2.1 Balanced Scorecards (BSCs)

As the aim of this paper is to create an information security framework based on the Balanced Scorecard (BSC), we build on prior research on the BSC, which is considered a well-established management scorecard in business practice. A study on the application and popularity of different management instruments in different economic regions ranked the BSC as fifth popular management instrument worldwide. Within the EMEA economic region (Europe, Middle East and Africa) the BSC was identified to be the most popular management instrument [12]. The usefulness of the BSC method was demonstrated for a variety of entities and different organizational settings including, e.g., higher education [13], national health service [14], banking [15] and public sector [16]. Another study conducted a systematic comparative research to relate the value of the BSC, and the value of specific elements of it, to the context of the application [17]. The BSC appeared to be of value to all ten organizations analyzed (although in varying degrees).

The Balanced Scorecard (BSC) is a measurement system of an entities' performance linking strategic objectives and measures across four different perspectives, and promising strategy mapping between each of these perspectives [9, 10]. The original standard dimensions describe how the *Learning and Growth* dimension (often also referred to as future perspective) feeds into the *Internal Business Process* and *Customer* dimensions, which impact the *Financial* dimension. The idea of a BSC is to find a set of measures that maintain a balance between different dimensions or characteristics, such as financial and non-financial aspects, short- and long-term objectives, lagging and leading indicators, and internal and external performance perspectives [11, 14]. These measures should not only give an overview of the current or actual state of an entities' situation, but also the desired or planned state in terms of specific targets. The gap between the actual against the planned state is the performance gap, which should be closed in a certain time with an action plan that is structurally linked with the according measures in the scorecard.

However, there are also critical reflections of the BSC [18, 19]. Some scientists question the causality between different perspectives and their suitability to monitor technological developments [19]. In the IT area the BSC was applied for e.g. strategic information systems [20], in the ERP [21] and IT governance [22] contexts, and for e-business development [23]. Linked or cascading Balanced scorecards were, for example, used in IT performance management with a developmental and operational BSC [22]. In the context of *organizational security*, the BSC has been transformed into an IT security scorecard [8, 24]. While some guidelines for the general transformation of the BSC into the IT security context were given, specific guidelines on how to design and implement metrics for different levels and characteristics of measurements are generally missing.

Due to its high diffusion rate in practice, the BSC seems to be an appropriate management instrument to capture and compare information security if it is adapted in structure and content to the specific requirements.

2.2 Security Scorecards and Recommendations

For the composition of the information security framework, scorecard based approaches and general recommendations about information security management (ISM) were taken into consideration. None of the identified sources were able to fulfill our requirements directly, however the choice of a BSC as basis model for our framework scorecard approach was supported and some of its subdomains were motivated.

The study of de Oliveira Alves, et al. [25] considers the governance of information security and therefore puts its primary focus on the strategic orientation. Their model is also based on the basic BSC and proposes indicators which are derived from best practice and which are also part of the CobiT and ISO/IEC 17799 frameworks. The BSC concept also constitutes the foundation of the ISScoreCard of Huang, Lee and Kao [24] which covers information security management of the manufacturing industry. Measures for enhancement of security awareness and resilience against attacks are assigned to their potential perspective. The BSC model for information security by Herath et al [8] seeks to implement performance management in relation to IT security. The BSC study of Royer and Meints [26] covers identity management and is inspired from the IT Infrastructure Library (ITIL) [27], CobiT [28] and other best practice sources. The “Cybersecurity Health Check” system [29] is also based on a BSC concept. Its aim is to determine information security by regarding the human factor, especially measures for awareness building and training of information security. This focus is anchored on the assumption that the human factor poses the weakest link of a cybersecurity chain [29]. Another BSC based study applies selected metrics with regard to ITIL, ISO/IEC 28002 and CobiT [30] for assessing the quality of information security for web-services.

Two internationally accepted frameworks in the domain of information security (NIST 800-55 and ISO 27001) have high relevance for the information security domain. NIST disseminated various publications that are dedicated to information security on different levels [31]. The NIST publication 800-55, for example, addresses the performance evaluation of information security and proposes a three-step ascertainment of a target level [32]. The ISO published a series of standards on the topic information security under the family name ISO 27000. Whilst ISO 2700 offers a general overview about management systems for information security, 27001 is dedicated to the requirements for the establishment, operation, surveillance, maintenance and continuous improvement of an information security management system (ISMS). ISO 27002 is built on ISO standard 27001 and deals with essential activities for creating and implementing a working ISMS.

3 Research Approach and Process

This study presents a designed, developed, and field-tested assessment framework that followed the Design Science Research (DSR) approach by Peffers et al. [33]. Accordingly, the research process was structured by the process steps given in Table 1. The three DSR cycles presented by Hevner [34] have been used to support different steps in the research process.

Table 1. Research Approach and Process based on Design Science [33]

Research Process	**Relevance Cycles**	**Design Cycles**	**Rigor Cycles**	**Events/ Methodology**
(1) Identify the problem and motivate	With application domain experts (consultants, information security experts)	n/a	With academic and practitioner literatures	Workshop 1
(2) Define Objectives of a Solution		Internal and external cycles. External cycles with application domain experts (consultants, information security experts)		Workshop 2
(3) Design & Development				Workshops 3-4
(4) Demonstration	With Chief Information Security Officers (CISOs)		n/a	Pre-Tests
(5) Evaluation	With CISOs		n/a	Face-To-Face Interviews
(6) Communication	With policy makers and application domain experts	n/a	n/a	Presentation event

For the first stage to “(1) Identify the problem and motivate”, we met with industry consultants and security experts from the application domain to clarify the problem and motivation for this research (workshop 1) followed by a consultation of academic and practitioner literatures. This led to the consideration and adaptation of the BSC concept to the security context. Thus, we engaged in relevance and rigor cycles, respectively. For the second stage to “(2) Define Objectives of a Solution”, we engaged again with representatives from the application domain (workshop 2) to engage in another relevance cycle. Next, we engaged in “(3) Design & Development” and revised our framework through internal and external design cycles. The third activity covers the design and development of an artifact, including a description of the artifact’s desired functionality [33]. Again, the external design cycles were supported by workshops (3-4) together with industry consultants and security experts. The stage “(4) Demonstration” was implemented by pre-testing the framework and meeting again to engage in another design cycle with the same domain experts. Activity four requires the demonstration of the use of the artifact to solve the problem, followed by an evaluation of its performance. The “(5) Evaluation” stage took place between June/2014 and October/2014 in terms of one-hour face-to-face interviews with 30 organizations, and was followed by another minor design cycle. After analyzing the results, we engaged in “(6) Communication” in terms of a formal event, where we presented and discussed the results together with policy makers and application domain experts.

4 Objectives, Design and Development of the Framework

4.1 Objectives of a Solution

The ISM assessment framework is intended to be a multidimensional, indicator based, information security assessment system for critical infrastructure companies taking ideas from the BSC. The most essential difference is that the BSC requires a very specific context, while we seek to develop a universal instrument to compare the cyber security states of critical infrastructure organizations (objective 1). This is the first among five general objectives that were identified as being essential in order to meet the specific requirements of this study (see Table 2). These general objective were identified as a result of the first workshop.

Table 2. Five General Framework Objectives

Objectives	**Description**
1) General applicability	The framework has to be equally applicable for companies in the critical infrastructure sector.
2) Representation of the whole organization	The choice of perspectives and multi objective definition should provide a complete representation of the whole organization.
3) Expressiveness of sub-dimensions	Sub-dimensions should have sufficient expressiveness to identify strengths and weaknesses in order to allow for corrective measures.
4) Multidimensional measurability on homogenous scales	Each sub-dimension is represented by multiple indicators that sufficiently describe the sub-dimension with homogenous scales. Indicators need to be defined in a way that exhaustively covers the sub-dimension on desired abstraction levels.
5) Aggregation of sub-dimensions	All sub-dimensions need to be aggregable with prior defined criteria in order to enable statements on different abstraction levels as well as to provide a holistic overall assessment.

The arrangement of perspectives allows communicating the overall situation. Therefore a precise definition and appropriate amount of different, correlating, multiple dimensions and targets of security relevant factors in terms of multi criteria decision making is necessary [35]. The measurement of scorecard dimensions is thus based on multiple modular subdomains. An aggregation of all measurements of an individual subdomain enables an overall statement of a dimension. This results in different abstraction layers.

The representation of an individual dimension provides an overview, whilst the inspections of individual and manageable sub-dimensions allows for more detailed insights, which can then be used in order to take measures [36].

An essential restriction for the choice of indicators is their measurability. The amount of indicators for describing the sub-dimensions may vary, a higher amount of indicators for a sub-dimension does not attach more value to it, but reduces the error of measurement. In order to summarize multiple indicators, scales are defined. Scaling schemes allow for quantitative measurement of different dimensions which were measured qualitative. Scales are measurement instruments that are used to numerically identify a relative amount, position or the presence or absence of a relevant unit [37]. As indicators serve as basic elements, their proper definition is of high importance.

In order to receive an easy to describe result it is necessary to group results starting on indicator levels to gradually reach a higher abstraction level. (See Figure 2). For an easy aggregation of the measurement results of individual sub-dimensions, it is necessary that they are balanced. Within the dimensions, their relevant indicators are condensed to index values. For this aggregation, different approaches can be applied dependent on knowledge and measurability of indicators. A unidimensional evaluation method condenses all sub-dimensions of the framework to a single main-dimension. This method, however, leads to a loss or falsification of information. Additionally, sub-dimensions are not independent or mutual exclusive, what may result in a distortion. Nevertheless, the instrument is useful to classify the given degree of achieved information security of a single organization or a group of organizations.

4.2 Framework Design

The ISM assessment framework consists of four main dimensions that are illustrated in Figure 1. The first dimension was called Security Ambition (SA) and refers to the potential or future perspective of the BSC. The second dimension is called Security Process (SP) and is based on the internal process perspective of the BSC. The third Resilience (RE) perspective is based on the customer perspective of the BSC. Finally, the Business Value (BV) refers to the financial or value perspective of the BSC. These dimensions and their reasoning are described next.

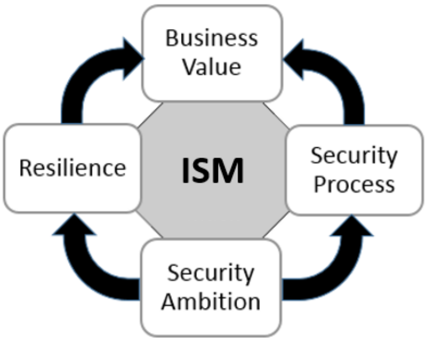

Fig. 1. Structure of the Information Security Management (ISM) assessment framework

According to NIST recommendations [31, 32], we included security guidelines as a starting point which are usually realized through an information security policy (ISP). This requirement is covered by the perspective “Security Ambition” within our model. As second pillar, NIST proposes to incorporate efficiency and effectiveness of the information security processes. The third pillar of NIST 800-55 covers security incidents that are directly influencing the business or mission level. This is covered by the perspective “Resilience”. It is also important to assess whether the critical infrastructure organization itself realizes what additional benefit information security offers. This is realized within the “Business Value” dimension of our framework. This approach does not only cover the recommendations of the basic balanced scorecard concept, but additionally takes into consideration that investment in information security requires transparency on cost and value side alike. Table 3 shows how these different dimensions can be related to other studies or frameworks from literature.

Security Ambition

This dimension covers all strategic and future-oriented ambitions to preserve or raise the security level of an organization. This includes primarily organizational factors (such as existence and quality of information security regulations and risk management), as well as procedural efforts in the domain of security awareness, training and education. The area of knowledge management covers the ability of an organization to assess development and outcome of new technologies. This ability is an essential requirement to be able to respond adequately to former unknown threats. In terms of general BSC dimensions, this category represents the future perspective [9] and takes the fundamental importance of the information security policy according to NIST 800-55 [31, 32] into account.

Security Processes

This dimension covers the efficiency and effectiveness of relevant information security processes of an organization. It is composed of the sub dimensions: information security management systems (ISMS) [38], patch management, change management, identity and access management, asset management, monitoring and reporting, as well as incident management and related cause research and problem analysis. In reference to the NIST 800-55 framework [31, 32], this dimension represents the “effectiveness/efficiency metrics of security service delivery” which assesses whether the security measures were implemented properly, perform as expected and deliver the expected outcome. NIST defines effectiveness as the robustness of the result itself and efficiency as the timeliness of the result [32]. According to the BSC logic, the quality of internal processes is examined, which are mapped by information security processes in the context of this study [9].

Resilience

The resilience perspective determines an organization’s resilience in regard to the required availability of service levels. This is of utterly importance for critical infrastructure organizations. An organization’s ability to maintain its service delivery mainly depends on how well the incident management is realized and how often and rigorous audits and security analysis are realized. In order to be able to react on changes in the availability of service, an emergency conception is required. It is thereby relevant how well the conception is internalized and how well relevant contractual partners are incorporated into this conception. Mapped to the BSC logic [9], resilience equals the customer perspective. The resilience perspective is further supported by the third pillar of the cybersecurity framework of NIST [31].

Business Value

This dimension reflects how much value an organization attaches to security. It captures how well information security is measured. The outcome as result of the measurement is not the main focus of this dimension, but the efficiency and effectiveness of the measuring system itself. The performance in this dimension shows whether an organization has knowledge about, measures and operates its own information security level. Additionally it is important to assess whether the costs and the value of information security are transparent. The NIST 800-55 recommendation [32] is therefore complemented with a dimension that, in terms of BSC logic, reflects the financial respectively the value perspective [9].

4.3 Aggregation

Frameworks in ICT evaluation and management are usually based on additive value models. These models use multiple (often conflicting) attributes to maximize a single quantity called utility or value. To aggregate single utilities and generate a super scale or index, multiple single-attribute value functions are aggregated. This is most regularly achieved by a simple additive weighting procedure [39], for example, in the Utility Ranking or Value Method [40]. The aggregation is undertaken by a weighted sum of single-attribute value functions. In the weighted sum method the overall suitability of each alternative is thereby calculated by averaging the score of each alternative with respect to every attribute with the corresponding importance weighting.

A value aggregation is possible on each level as all values should represent independent, unified and normed target values of the given company. This procedure is called value-synthesis in context of utility analysis [40]. For aggregation of the data different approaches can be applied, for example the Profile Distance Method [41]. A common method is to use a weighted average with normalized indicator values [36]. Normalization in this context refers to adjusting measurements on different scales to a uniform scale. It should be noted that aggregation leads to information losses and bias.

If there is no information available for weighting, it is advisable to use a simple average, without weighting. This results in average values for each group. Our model uses a hierarchical indicator model and assumes each hierarchical level to be equally weighted. That means that each abstraction level aggregates values independent of the amount of indicators with the same weight into the aggregation. Due to easier handling and comprehensibility it is common to use a linear aggregation method. However, this assumes that all values are compensable with each other, which is does not hold in reality [36]. Individual evaluation criteria represent different features which, in sum, allow for an extensive and holistic evaluation of the information security level of a participating company.

Table 3. Models and Frameworks Related to ISM Framework Dimensions

Reference	**Dimensions (Number of indices)**	**Framework**
Enterprise Security Governance - Security Dashboard [25]	Risk Management (6)	SA
	Policy Compliance (10)	SA, BV
	Asset Management (5)	RE
	Knowledge Management (8)	SA
	Incident Management (7)	RE
	Continuity Management (10)	SP
	Security Infrastructure (8)	SP, BV
Security Performance (BSC) [24]	Financial (5)	BV
	Customer (5)	RE
	Internal process (11)	SP
	Learning & growth (14)	SA
Enterprise Identity Management [26]	Financial/monetary (3)	BV
	Business process (3)	SP
	Supporting process and ICT infrastructure (3)	SP
	Information security, risk and compliance (3)	SA, BV
Cybersecurity Health Check [29]	Protection Requisitions (2)	SP, BV
	Defense-in-Depth Implementation (3)	SP
	ISMS Establishment (4)	SA
	Security Awareness & Education (3)	SA
Quality of Service Security [30]	Compliance (0)	BV
	Integrity (0)	RE
	Reliability (0)	RE
	Availability (2)	RE
	Confidentiality (3)	SP
NIST Publication 800-55 [31, 32]	Implementation of security policy	SA
	Effectiveness/efficiency metrics of security services delivery	SP
	Impact metrics of security events on business/mission level	RE
ISO/IEC 27001/2 (ISO 17799) [38, 42]	Security policy	SA
	Organizing information security	SA
	Asset management	SP
	Human resources security	SP
	Physical and environmental security	SP
	Communications and operations management	SA
	Access control	SP
	Information security acquisition development & maintenance	RE
	Information security incident management	RE
	Business continuity management	SA
	Compliance	BV

The hierarchical levels of the index are visualized in Figure 2. The numbers in the brackets refer to the number of questions within the questionnaire. The black boxes display the sub-dimension-indexes, which together form the dimension-index. In total, the scorecard is made up of 108 indicators that are grouped to 19 sub-dimensions which are subsumed to four main dimensions that finally form the overall index.

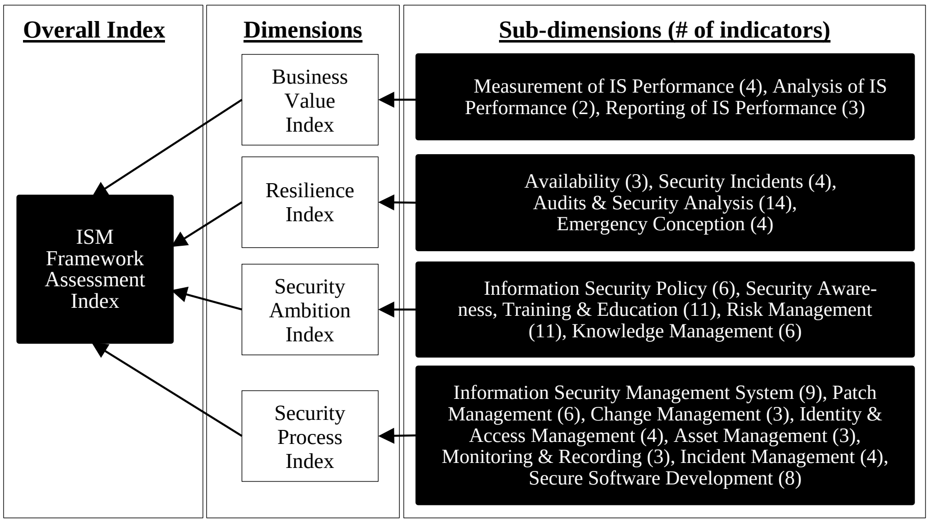
Overall Index
Dimensions
Sub-dimensions (# of indicators)
ISM Framework Assessment Index
Business Value Index
Resilience Index
Security Ambition Index
Security Process Index
Measurement of IS Performance (4), Analysis of IS Performance (2), Reporting of IS Performance (3)
Availability (3), Security Incidents (4), Audits & Security Analysis (14), Emergency Conception (4)
Information Security Policy (6), Security Awareness, Training & Education (11), Risk Management (11), Knowledge Management (6)
Information Security Management System (9), Patch Management (6), Change Management (3), Identity & Access Management (4), Asset Management (3), Monitoring & Recording (3), Incident Management (4), Secure Software Development (8)

Fig. 2. Hierarchical levels of the ISM framework

5 Framework Demonstration and Evaluation

The developed information security framework included contextual questions, which were used to enable an additional qualitative assessment alongside the quantitative assessments needed to create aggregate values (indices).

5.1 Pretests

Upon finalization of the framework and the underlying questionnaire, two pre-tests were carried out. The main aims of these pre-tests was to test the framework's measurement instrument via structured face-to-face interviews in real-life environments and demonstrate the validity of the instrument. It was tested whether the instrument is comprehensible and how much time it takes to answer all questions diligently. For this test run it was particularly interesting to understand whether the target person of the interview, the Chief Information Security Officer (CISO), could answer all questions by herself without consulting an additional knowledge source (colleagues or a database).

The result of these pre-tests was used to further refine the questionnaire. It was necessary to optimize the length of the questionnaire considering the time limitations to complete it. All questions that could not be answered or were likely to need a preparation time to be answered were removed. The pretests also demonstrated that is was necessary to add some more contextual questions in order to avoid misinterpretation of some index values. After all adjustments were made, a second round of pre-tests was carried out. The findings of this round did not require further refinements of the structured questionnaire. Therefore the research instrument was found to be ready to be employed.

5.2 Framework Evaluation

The data collection process with face-to-face interviews alongside a structure questionnaire was conducted during the time period from June 2014 to October 2014 in Austria. In total, 30 companies participated, eight companies of the information and communication technology industry, six companies of the energy supply sector, six transportation companies, four within the banking sector, three from the health care sector and three from other industries. Although the number of participants was not very high, a better part of Austrians critical infrastructure companies were covered.

The questionnaire comprises 108 indicators in total, 34 indicators for the dimensions "Security Ambition", 25 indicators for the Dimension "Resilience", 40 indicators for the dimension "Security Process" and 8 indicators for the dimension "Business Value". Additionally, the questionnaire uses descriptive complementary questions in open and semi-structured form. All indicators are assessed with a 5 point Likert scale with interval scaled answers ranging from 1 (excellent) to 5 (insufficient). This common scale allowed for the required uniform understanding of questions by all participants. It was openly stated to give a critical self-assessment and provide a satisfaction level for these questions. The questionnaire also comprises some contextual questions that allow for a qualitative assessment. For example the value of IT security is measured by considering the allocation of financial resources that are directly associated with service delivery of security management.

6 Discussion and Conclusion

This paper proposed the development of a general framework for assessing the quality of information security management driven by the needs of understanding the comparative levels of cyber-security of critical infrastructure organizations. A preliminary literature research identified the BSC as a useful base model for developing such a framework due to its wide recognition in practice, literature, its overall comprehensiveness and strategic management orientation. A design science research (DSR) approach based on the six stages by Peffers et al. [33] was used to develop an information security framework, which took into account three DSR cycles presented by Hevner [34]. These cycles assured relevance, rigor and effective design principles. In particular, we involved subject experts and CISOs as the main stakeholders from the information security domain. The DSR research process was concluded with a presentation to all stakeholders including many of the interviewed CISOs, policy makers, and security and critical infrastructure industry experts.

The resulting information security framework is deemed capable of realizing a general information security status evaluation, which can be used to compare critical infrastructure organizations. For this purpose, we used a range of 108 indicators that are grouped to 19 sub-dimensions. However, in order to give these metrics additional meaning and support understanding, it was necessary to complement the quantitative questions with open qualitative questions that capture the special contextual situations. More precisely quantitative evaluation serves to benchmark, whereas qualitative questions can be used to explain and interpret scores. The scorecard in terms of the quantitative estimators alone does not portray the complete security status. An example for an open question is „Who reports to the management? – Describe the reporting structure". In contrast, a typical index question consists of an evaluation of the quality of, for example an emergency concept, and the significance that is given to it by upper (business level) management.

An important issue that needs to be clarified prior to the application of the assessment framework, is to accept it as comparative learning and assessment tool to reveal relative weaknesses and strengths. As the questionnaire is based on a self-assessment, it would easily be possible to whitewash potential problems. This has to be clarified prior to its implementation on the organization and individual levels. As the CISO is the main target person for the questionnaire, she is prone to experience a social desirability bias. This bias refers to the tendency to give socially desirable responses [43].

Future work could include an evaluation of possible social desirability bias in order to control it in data analysis. A further enhancement would be an incorporation of companies' resource dependencies in regard to cyber-security. This would result in a more holistic view. It should be possible to cascade the framework for multiple companies. Other future research could extend our work by comparing the proposed framework with others in terms of applicability and accuracy. The proposed framework needs a constant refinement in terms of both structure and suggested metrics that can be applied throughout all different sectors within the critical infrastructure sector to allow for comparisons. Additionally, different aggregation approaches could be used, in particular to account for different weighting profiles.

Acknowledgment. We would like to thank Michael Stephanitsch for conducting the interviews and especially Wolfgang Gattringer, Heiko Borchert and Wolfgang Rosenkranz for hosting the workshops and engaging in the discussions.

7 References

1. Gottwald, S.: Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure European Commission (2009)
2. Hare, F.: The Cyber Threat to National Security Why Can't We Agree? Conference on Cyber Conflict Proceedings 15 (2010)
3. COUNCIL DIRECTIVE 2008/114/EC. EU (2008)
4. Gercke, M.: Understanding Cybercrime: A Guide for Developing Countries. In: Division, I.A.a.C. (ed.), (2011)
5. Vaughn Jr, R.B., Henning, R., Siraj, A.: Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp. 10. (2003)

6. Fink, G., O'Donoghue, K.F., Chappell, B.L., Turner, T.G.: A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems. Proceedings of the 16th International Parallel and Distributed Processing Symposium, pp. 17. IEEE Computer Society (2002)
7. Bernroider, E.W.N., Koch, S., Stix, V.: A comprehensive framework approach using content, context, process views to combine methods from operations research for IT assessments. Information Systems Management 30, 75-88 (2013)
8. Herath, T., Herath, H., Bremser, W.G.: Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. Information Systems Management 27, 72-81 (2010)
9. Kaplan, R.S., Norton, D.P.: The Balanced Scorecard - measures that drive performance. Harvard Business Review 70, 8 (1992)
10. Kaplan, R.S., Norton, D.P.: Putting the Balanced Scorecard to Work. Harvard Business Review 71, 14 (1993)
11. Kaplan, R.S., Norton, D.P.: The Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press (1996)
12. Rigby, D., Bilodeau, B.: Management Tools & Trends 2013. Bain & Company (2013)
13. Lawrence, S., Sharma, U.: Commodification of Education and Academic LABOUR—Using the Balanced Scorecard in a University Setting. Critical Perspectives on Accounting 13, 661-677 (2002)
14. Protti, D.: A proposal to use a balanced scorecard to evaluate Information for Health: an information strategy for the modern NHS (1998–2005). Computers in Biology and Medicine 32, 221-236 (2002)
15. Littler, K., Aisthorpe, P., Hudson, R., Keasey, K.: A new approach to linking strategy formulation and strategy implementation: an example from the UK banking sector. International Journal of Information Management 20, 411-428 (2000)
16. Irwin, D.: Strategy Mapping in the Public Sector. Long Range Planning 35, 637-647 (2002)
17. Southern, G.: From Teaching to Practice, via Consultancy, and then to Research? European Management Journal 20, 401-408 (2002)
18. Ahn, H.: Applying the Balanced Scorecard Concept: An Experience Report. Long Range Planning 34, 441-461 (2001)
19. Norreklit, H.: The balance on the balanced scorecard a critical analysis of some of its assumptions. Management Accounting Research 11, 65-88 (2000)
20. Martinsons, M., Davison, R., Tse, D.: The balanced scorecard: a foundation for the strategic management of information systems. Decision Support Systems 25, 71-88 (1999)
21. Roseman, M., Wiese, J.: Measuring the Performance of ERP Software – a Balanced Scorecard Approach. Australasian Conference on Information Systems 10 (1999)
22. Grembergen, V.: The Balanced Scorecard and IT Governance. Information Systems Control (2000)
23. Bernroider, E.W.N., Hampel, A.: An Application of the Balanced Scorecard as a Strategic IT-Controlling Instrument for E-Business Development. International Conference on Electronic Business, Singapore (2003)
24. Huang, S.M., Lee, C.L., Kao, A.C.: Balancing performance measures for information security management. Industrial Management & Data Systems 106, 242-255 (2006)
25. de Oliveira Alves, G.A., da Costa Carmo, L. F. R., Almeida, A.C.R.D.: Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG). Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on, pp. 71-80 (2006)

26. Royer, D., Meints, M.: Enterprise Identity Management – Towards a Decision Support Framework Based on the Balanced Scorecard Approach. Bus. Inf. Syst. Eng. 1, (2009)
27. TSO: Introduction to the ITIL service lifecycle. The Stationary Office (TSO), Office of Government Commerce (OGC), Belfast, Ireland (2010)
28. ISACA: COBIT - 4th Edition. Information Systems Audit and Control Foundation, IT Governance Institute, Rolling Meadows, USA (2007)
29. Pan, M.S., Wu, C.-W., Chen, P.-T., Lo, T.Y., Liu, W.P.: Cybersecurity Healt Check. In: Andreasson, K. (ed.) Cybersecurity: Public Sector Threats and Responses, pp. 392. CRC Press (2012)
30. Charuenporn, P., Intakosum, S.: Qos-Security Metrics Based on ITIL and COBIT Standard for Measurement Web Services. Journal of Universal Computer Science 18, 24 (2012)
31. NIST: Framework for Improving Critical Infrastructure Cybersecurity. (2014)
32. Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., Robinson, W.: NIST Special Publication 800-55 Information Security. NIST, Gaithersburg (2008)
33. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems 24, 45-77 (2007)
34. Hevner, A.R.: A three cycle view of design science research. Scandinavian journal of information systems 19, 4 (2007)
35. Bernroider, E.W.N., Mitlöhner, J.: Characteristics of the Multiple Attribute Decision Making Methodology in Enterprise Resource Planning Software Decisions. Communications of the IIMA 5, (2005)
36. Merz, M.: Entwicklung einer indikatorenbasierten Methodik zur Vulnerabilitätsanalyse für die Bewertung von Risiken in der industriellen Produktion. KIT Scientific Publishing (2011)
37. Atteslander, P.: Methoden der empirischen Sozialforschung. Erich Schmidt Verlag (2008)
38. ISO/IEC: The ISMS family of standards (2700X). Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques (2014)
39. Yoon, K.P., Hwang, C.-L.-. Multiple attribute decision making: An introduction. Sage University Paper series on Quantitative Applications in the Social Sciences. Thousand Oaks, CA: Sage (1995)
40. Zangemeister, C.: Nutzwertanalyse in der Systemtechnik. Wittemann'sche Verlagsbuchhandlung, München (1976)
41. Bernroider, E.W.N., Stix, V.: Profile distance method - a multi-attribute decision making approach for information system investments. Decision Support Systems 42 988-998 (2006)
42. Sahibudin, S., Sharifi, M., Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. Second Asia International Conference on Modeling & Simulation, 2008. AICMS 08. , pp. 749-753 (2008)
43. Grimm, P.: Social Desirability Bias. Wiley International Encyclopedia of Marketing. John Wiley & Sons, Ltd (2010)