BORIS –Business ORiented management of Information Security

Sebastian Sowa[1], Dr. Lampros Tsinas[2], Prof. Dr. Roland Gabriel[3]

[1] Institute for E-Business Security (ISEB),
Ruhr-University of Bochum, GC 3/29, 44780 Bochum, Germany
ssowa@winf.rub.de

[2] Munich Re, Koeniginstr. 107, 80802 Munich, Germany
ltsinas@munichre.com

[3] Chair of Business Informatics
Ruhr-University of Bochum, GC 3/132, 44780 Bochum, Germany
rgabriel@winf.rub.de

Abstract. The present paper aims to successfully deal with the needs of information security functions by providing a management tool which links business and information security objectives. In the past terms, information security has become fortunately a top management topic due to the recognition of the continuously increasing dependencies of the overall business success on secure information and information processing technologies and means. While the focus of information security management primary lay on the implementation of solutions to assure the achievement of the enterprises' security objectives and their management, the business oriented management objectives were typically not regarded as major concern. Today, information security management executives are severely confronted with a different situation. An increasing pressure forces them to manage the security measures not only using their security but also business glasses. To handle this challenge, a framework is presented in this paper. It supports any information security functions with a strong economic focus whereby it specifically links business and information security objectives. The core of the presented methodology has proven to be reliable, user friendly, consistent and precise under real conditions over several years.

Keywords: information security management, information management, strategic management, business objectives, business alignment, business IT alignment, financial management, financial balancing, optimization, return on security investment, value based management, balanced scorecard, performance management, security metrics, KPI.

1 Introduction

1.1 Background

Because of community's increasing dependency on secure and private information, the establishment and continuous management of information security today is one of the most challenging tasks [La05; La95]. Several models, methods and measures were introduced in the past each covering particular aspects of the subject of matter. Most of the approaches focus primary technical issues but also business oriented approaches for managing information security raised in interest in the recent past.

A wide range of economic approaches have then been presented what indicates the increasing interest in security management methods with an economic focus (i.e. [AM06; CW04; GL02; GL04; So02]). But many of these approaches mainly focus on narrow and specialized fields without meeting the challenges of a holistically integrated concept. They especially lack in integrating the high number of different actors and their interests that the enterprise's information security system contains. And even more important, they lack in establishing a systematic method that directly and transparently links business with information security objectives and measures as well as the information security objectives and measures with a method for defining optimal investment policies. To handle these challenges, a framework for managing information security with a strong economic focus is presented in the following paragraphs. To set the record straight from the beginning, this task starts with the clarification of the appreciation of used terms and intended goals.

1.2 Terms

Information as the first relevant term used in the discussion of information security management topics can linguistically be derived from the Latin informatio. Informatio in this turn stands for explanation or interpretation of ideas as well as it can be used in the meaning of education, training or instruction what gives a first consideration about an accurate and precise definition: Information in this paper is defined as an explanatory, significant assertion that is part of the overall knowledge as well as it is seen as specific, from human beings interpreted technical or non-technical processed data [BMR00; GB03]. This definition is precisely in line with the ISO/IEC standards which explain that information "can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation" [ISO05a; ISO05b]. This – mostly trivial – way to use the term information unfortunately does not reflect the common sense in the information security community. There, it is quit often assumed to only affect electronic data, and thereby information security management has mostly to deal with IT. In this paper, we clear focus on a broad and comprehensive denotation, which the described methodology has to deal with.

As consequence of the appreciation of information, also information security has to cover technical as well as non-technical challenges. In this context, the ISO explains that whatever “form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities” [ISO05a; ISO05b]. As seen in the citation, the standard explicitly accentuates the importance of the link of information security to business management what leads to the first of the requirements that are defined for the business oriented information security management framework presented in this contribution. This requirement and others are described in the following.

1.3 Goals

As information security is seen as business and strategic management topic, the information security management framework then has to enable executives to transparently link business to information security objectives (R1). Therefore, the framework should support to answer top management’s questions about information security performance as well as it should support information security management to address areas suitable or necessary to improve the performance influencing indicators (R2).

Shifting the view to the information security management itself, more detailed information is typically needed. From this background, the framework should support the process of defining concrete and measurable indicators for the security target as well as for the current state in different levels of detail (R3).

To close identified gaps by planning, introducing and managing adequate measures and programs, especially investment decisions have to be addressed in the context of the regarded business oriented management framework. The framework should support the executives in the processes of finding and defining cost benefit balanced investment strategies (R4).

Wherever and whenever investments are done and measures are already running, the framework should include a method for evaluation that can be used for the task of optimizing the economic and strategic performance of the overall information security infrastructure (R5).

As last requirement at this point, the evaluation and optimization process as well as the other named aspects of the management framework have to be integrated into a management process that enables the continuously and especially sustainable business oriented information security management (R6).

The defined requirements base on individual interviews with information security management executives and are additionally in line with findings in several topic-near publications like [Ca04; CCR04] for instance.

2 BORIS design

2.1 Overview

The framework meeting the described requirements and presented in this contribution is the result of the evolutionary advancement of the management approach presented in [KSST07]. It consists of four layers whereby each layer covers particular aspects of strategic, tactical and operational (STO) challenges. As seen in Fig. 1, the top level focuses on the business and information security management interaction, the second layer deals with linking the results of the strategic methods to specific information security objectives as well as it supports to address the current state. The third layer replenishes the tactical methods as it deals with defining a balanced investment policy for implementing and managing measures targeted to close identified gaps. Because of the strong interdependencies of the second and third layer in regard to the financial alignment, they are combined in the so called Cost-Benefit-Toolbox (CB-Toolbox) which also contains elements of the fourth layer. The fourth layer holds tools for the evaluation and optimization of an information security infrastructure what closes the STO view. A program management cycle rounds the framework of.

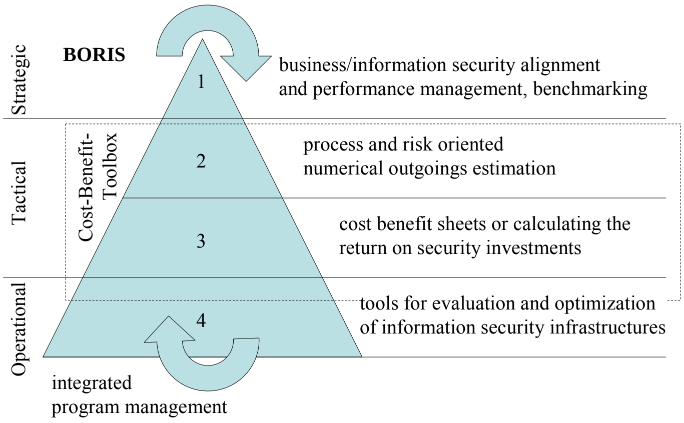

Strategic
BORIS
1
business/information security alignment
and performance management, benchmarking
Tactical
Cost-Benefit-Toolbox
2
process and risk oriented
numerical outgoings estimation
3
cost benefit sheets or calculating the
return on security investments
Operational
4
tools for evaluation and optimization
of information security infrastructures
integrated
program management

Fig. 1. BORIS general topology

2.2 Business strategic methods

As visualized, the top layer of the framework deals with business/information security alignment and performance management. It consists of a transferring system for linking strategic as well as compliance driver to information security objectives and a central scorecard system with which the performance can be measured (s. Fig. 2).

The theoretical basis of the scorecard system is laid by the Balanced Scorecard which *Norton* and *Kaplan* have developed [KN96; KN05]. It provides a framework with which performance influencers are anchored in classically four dependent dimensions, each containing objectives, metrics, targets and measures. Historically, the multidimensional system of the Balanced Scorecard was established to overcome one of the main problems arising in measuring the original aimed overall enterprise performance on financial indicators: Because the traditionally solely used financial indicators only could reflect a small range of the entire performance influencers, they have been linked to customer and process indicators which again have been linked to indicators which visualize the dependency of the customer and process efficiency on the enterprise ability for learning and developing.

Beside the implementation of Balanced Scorecard systems in several branches and industries, the general idea was also recognized quite early in the field of information management (i.e. [GB02; GB03]) where information security sometime was even implemented as own, additional dimension [Ba01]. Other, proprietary systems (ISF; Information Security Forum) have adopted the original four axes end embedded information security objective therein.

Because of the aim of connecting the BORIS system with an enterprise Balanced Scorecard, the business strategic method defined in the BORIS framework integrates information security performance objectives and metrics in the traditional dimensions finance, customer, processes and future (similar to learning and development). An organization dimension is defined in addition aiming to match the requirements of several standards which accentuate the importance of organizational information security performance. The sixth dimensions then cover the importance of the technological information security infrastructure and address relevant performance indicators for the objectives. All sixth dimensions are connected through a knowledge-based steering methodology.

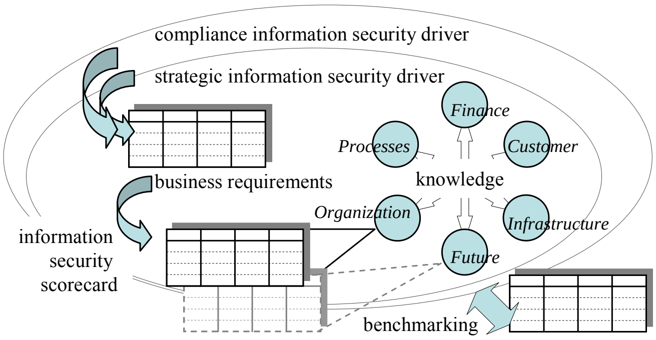

compliance information security driver
strategic information security driver
Finance
Processes
Customer
business requirements
knowledge
Organization
Infrastructure
information security scorecard
Future
benchmarking

Fig. 2. Conceptualization of business strategic methods

The compliance and strategic requirements are transferred to security objectives by the use of a systematic and formal defined process whereby relevant players such as the chief information officer, business process owners, and compliance officers have to cooperatively agree to. Transferring tables, containing columns for the business objectives and related security dimension and objectives, are offered to support the executives in the defining and agreement process. The table – based on the underlying process – propagates business requirements (formulated in "business language") to information security requirement without loosing the vital connection between them.

It is only this explicitly applied connector philosophy between business and ISMS that validates the right to exist to any security control.

When the business objectives are linked to security dimensions and transferred to concrete security objectives, metrics for the measurement of the level of objectives' fulfillment have to be defined as well processes have to be established for ensuring the continuously measure of the business aligned information security indicators. As example for the organization dimension that aims to answer the question about the organizational efficiency, objectives like the improvement of regulatory compliance with regard to the alignment of the information security organization structure to a specific standard like ISO/IEC 27001 or any other one the executives have defined in the objective transferring tables could be addressed [GSW08; KSST07].

The information security performance scorecard system itself enables the handling of quantitative but especially also qualitative metrics. Both types are brought into a balanced situation. The system can directly be linked to the entire enterprise performance scorecard system (if established) as well as the system can hierarchally be brought down as far as to the operational level of the enterprises' information security organization. Furthermore, the cascading character offers the use of an as flexible as expandable instrument that directly links business to information security objectives as well as it can help to link the resulting strategies with human individual objectives' systems. Thereby, the prerequisite agreement process regarding the definition of the security objectives ensures to overcome the limited view of an autonomous set of ever reachable objectives as well as it brings together the quantum of information security relevant players in an cooperative manner [Fi05].

Benchmarking at this point replenishes the set of strategic methods. It supports to identify the own level of maturity while the individual records of performance are set in relation to a peer group of interest for the enterprise. Benchmarking is widely used and accepted [Po07; Xe87]. The method offers to benefit from the results if the data is correctly interpreted and the peers are of adequate competitive importance [La06; SCC07]. The key factor for success regarding the BORIS framework is to have a comprehensive database, a sophisticated model, and a clear focus to the subject of matter, namely information security what reduces the quantum of suitable as well as available benchmark platforms to only few ones [KSST07]. For the BORIS framework, the Information Security Status Survey provided for the members of and by the Information Security Forum (ISF) is currently used in this context.

To transfer benchmarking results to concrete improvement results, the strategies, objectives and identified gaps between the objectives and the current states in each of the six dimensions of the business/information security alignment and performance management method have to be linked to process tactical methods. These methods are anchored in the next layer of the BORIS framework and explained in the following.

2.3 Process tactical methods

While the first layer of the BORIS framework aims to answer the question about the alignment grade of the information security infrastructure with business and thereby including compliance requirements as well as relevant performance indicators are addressed for monitoring, the results are used for the information security concerned process tactical methods described in the following paragraphs.

The process and risk oriented numerical outgoings estimation (PRONOE) method as first one of the process tactical ones is introduced in detail in [Ts07]. It is directly linked to the introduced security strategic performance scorecard and fulfills a top-down as well as a bottom-up function: The performance objectives are used as operational guidelines while the data processed in PRONOE again is delivered up to the six dimensions of the strategic performance scorecard in an aggregated form. Fig. 3 shows that PRONOE contains three main components [KSST07]: A risk assessment layer for determining qualitative actual and debit states, the (100- X)% rule for determining the quantitative debit state and a process for the cost-benefit balancing comparison of the qualitative and quantitative actual and debit state values which especially supports to address financial investment policy goals that are then used by the financial tactical methods described in chapter 2.4.

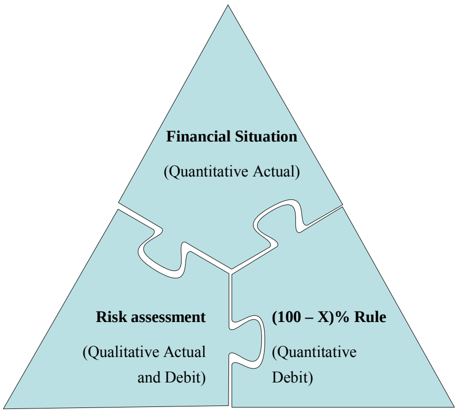


Fig. 3. PRONOE core components

As shown in the top layer configuration of the BORIS framework, a management forum should determine the security performance objectives what concretely means to agree on a specific level of acceptable risk exposure and on the areas which require additional risk controls. It is naturally not responsible for making explicit proposals for risk minimization/mitigation, as this is the domain of the security specialists who select appropriate controls (including security awareness programs [La07; Pe05]) in the context of establishing and maintaining suitable security architectures [SCL05].

The current security situation then is assessed using risk assessments or scorecard analyses instruments. The scorecard analysis practice in this context has been outlined by *Loomans* [Lo04] and is also part of the work of the Information Security Forum pertaining FIRM (Fundamental Information Risk Management) [ISF08]. It ultimately reflects a structured component for ascertaining current and target values in various risk areas (i.e. so-called R_i risk areas) and thereby follows the construct of the scorecard system established for the business strategic methods in layer one.

For practicality reasons, the scorecard system used for risk the assessment process should hold the dimensions up to a value of about ten. A desirable distribution of the dimensions thereby could use the structure of acknowledge standards like ISO/IEC 17799 [ISO05a], the CObIT framework [ITGI07] or any other theoretical affirmed or best practice bases. Currently, the five dimensions defined in the implemented version of the risk scorecard were derived from FIRM [ISF08]. They address:

- Criticality
- Level of threat
- Business impact
- Vulnerability – status of arrangements
- Vulnerability – special circumstances

As the second component of PRONOE, the (100- X)% rule transfers the level of the acceptable risk exposure agreed on by the members of the management forum to protection areas which are defined as 100 percent minus the accepted level of risk in percentage. It bases on the following rules:

- Each assertion about the acceptable risk level implicates directly that any further level of risk is not accepted
- As consequence, each assertion also defines the areas for investment in order to reduce the overlapping risk levels to acceptable ones

What directly follows out of the named rules is that the protection areas constitute the areas of investment. Therefore, they are used for investment decision making processes as well as they are linked to the next component of PRONOE – the cost-benefit balancing comparison of the qualitative and quantitative actual and debit state. For cost-benefit balancing comparisons, the quantitative actual situation has of course to be assessed first what is done for each risk area R_i. Completed, the result of the (then following) comparison enables information security management executives to visualize and analyze the total amount of information security relevant investments as well as those per risk area R_i. This, in turn, supports the determination whether the established security level could have been realized using the defined resources or whether an objective has been left unmet because sufficient resources were not available what as consequence supports to identify the so-called “money drains” as well as chronically under-funded areas [KSST07].

To sum up to this point, the first and second layer support the strategic alignment and performance measurement as well as they support to answer process tactical questions of information security interests. They hold up methods to transfer business to security objectives, to define information security protection areas and to evaluate the reached level of maturity. But for a holistic approach, two more questions have to be addressed, namely how to handle financial questions arising from process tactical results and how to handle optimization challenges at the operational dimension.

2.4 Financial tactical methods

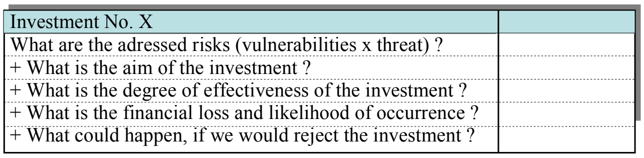
Whenever the process tactical methods result in the identification of protection areas where measures have to be implemented in order to reduce risks, questions about optimal investments on a more detailed level arise. Here, BORIS offers two general methods to support executives in decision making:

- Return on Security Investment (RoSI)
- Cost Benefit Sheets (CoBS)

Approaches for the definition of RoSI were highly recognized in the past due to the aspiration for having a method that could handle the problematic financial investment decision question. Its structure and goals are similar to the concept of the Return on Investment (ROI) used to justify traditional financial investment decisions. The calculation of a RoSI bases on four steps [WFCR01]:

1. Defining the Annualized Rate of Occurrence (ARO) for a specific risk
2. Identifying the Single Loss Expectancy (SLE) for the given risk
3. Determining the Annual Loss Expectancy (ALE) as product of ARO times SLE
4. Comparing the ALE without risk concerned security investment with the ALE if the investment is done plus the costs for this investment

The problem about RoSI is that it is only meaningful where the calculation bases on existent and statistically significant data [KSST07; Ti03]. In all other situations, when these data are missing, an equivalent methodology must be applied. In this case, Cost Benefit Sheets (CoBS) as shown in Fig. 4 can be used.



Investment No. X	
What are the adressed risks (vulnerabilities x threat) ?	
+ What is the aim of the investment ?	
+ What is the degree of effectiveness of the investment ?	
+ What is the financial loss and likelihood of occurrence ?	
+ What could happen, if we would reject the investment ?	

Fig. 4. Cost Benefit Sheet (CoBS) for information security investment

This approach is very much similar to the 5-Step approach introduced by *Schneier* in [Sc06]. In antithesis with this proposal, the CoBS model is characterized by a coherent schema, a well-sorted order which is reflecting the psychological aspects during the assessment, and is layered in that way, that a negative response of any layer leads directly to a rejection of an investment proposal.

Using CoBS, all existing data should theoretically be considered while completing the sheets. Here, a systematic documentation can enhance the CoBS quality as well as it enabled to appropriately justify but also revise investment decision. So what CoBS or the RoSI method can do is to justify and especially document investment decisions on the bases of BORIS process tactical results. On the other side, these methods especially link the risk areas R_i defined in PRONOE to the operational evaluation methods anchored in the next layer of the BORIS framework.

2.5 Operational evaluation and optimization methods

So far, strategic, process and financial tactical methods are introduced and linked to each other what demonstrates a closed chain from enterprise business to security business management. For rounding of the quantum of methods for the BORIS approach, the operational level of the presented framework holds methods for:

- Evaluating the current controls infrastructure (ECI)
- Optimizing the necessary controls infrastructure (OCI)

Whereas the aforementioned methods support to compare an actual and debit state regarding strategic performance respectively the risk-investment-ratio, the operational methods in the following support the comparison of the actual and debit states on the level of implemented and operationally running measures like physical or technical ones for instance. The methods base on the process for evaluation and control of IT risks which is introduced in detail by [Kl07; WK05] and which is also part of the first version of the approach presented in this contribution [KSST07]. Here, the originally to the German “IT-Grundschutz Catalogues” [BSI05] linked approach is structurally separated from the German standard and used as for FIRM aiming to better harmonize the different layers of the BORIS framework. Thereby, the methods make use of the Fuzzy-Sets-Theory introduced in detail by [Zi93; Zi01] for algorithmic.

As described before, the FIRM scorecard offers five dimensions each containing a questionnaire regarding different aspects of risk assessment. Thereby, the addressed controls are directly linked to the control areas of the ISF Standard of Good Practice for Information Security which in turn is aligned to ISO 17799 [ISO05a] as well as CObIT 4.1 [ITGI07]. Each of the currently six control areas contains sections. Each section again contains control objectives which can be used on an operational level of information security management. The set of control areas in the following is defined as *C*, the set of sections as *S*, the considered enterprise *e* is element of the set of overall enterprises *E*.

For ECI, the first step is to proof whether S_{ij} for $i = 1\ to\ N_j$ (N_j is the number of sections for control area *j*) and $j = 1\ to\ 6$ is relevant or expendable for the considered *e*. The identified individual relevant sections define the fuzzy set *R* as visualized through the following function:

$$\mu_R\,(S_{ij}, e) = \begin{cases} 1\ if\ S_{ij}\ is\ relevant\ for\ e \\ 0\ if\ S_{ij}\ otherwise \end{cases} \qquad \mathbf{(1)}$$

For each $r \in R$, it is crosschecked with the FIRM questionnaires, whether the required control is in place, in progress, planned or if nothing is done yet. With the aim of evaluating the actual set of controls, planned and not-started actions lead to the same result, namely that controls are not implemented. For this reason and with the background of the assumption that the identified not-started actions are followed by immediate planning activities, planned and not-started actions are regarded as one characteristic in the used algorithmic of the evaluation method. The result of this step shapes the fuzzy set of the implementation grade *G* with the function:

$$\mu_G\ (S_{ij}, e) = \begin{cases} 1 & \text{if } S_{ij} \text{ is completed} \\ 0{,}5 & \text{if } S_{ij} \text{ is in progress} \\ 0 & \text{otherwise} \end{cases} \qquad \textbf{(2)}$$

As only relevant sections are regarded, the average out of *R* and *S* defined using the minimum operator then gives the fuzzy set for the section status *SG* [WK05]:

$$\mu_{SG}\ (S_{ij}, e) = \{\ \min\ \ \mu_R\ (S_{ij}, e);\ \mu_S\ (S_{ij}, e)\ \}\ \ \forall\ e \in E,\ \ S_{ij} \in S \qquad \textbf{(3)}$$

In the next step of the evaluation process, the importance of the individual sections for the specifically considered *e* are addressed by matching the security performance objectives set in the upper layers of the BORIS framework with the risk assessment results specially focusing on the criticality, level of threat and the business impact of the regarded information resource. According to the FIRM process, a classification of five characteristics is chosen: Very high (A), high (B), medium (C), low (D), and very low (E). On the bases of this classification, the degree of importance of each section is determined resulting in the functions for the fuzzy sets $\mu_A\ (S_{ij})$, $\mu_B\ (S_{ij})$, $\mu_C\ (S_{ij})$, $\mu_D\ (S_{ij})$, and $\mu_E\ (S_{ij})$ each containing the value of 1 if S_{ij} is classified or O if S_{ij} is not classified as A respectively B, C, D, or E section.

For each control area *C*, μ_{SG} with regard to A- to E-sections is set in relation to μ_A to μ_E what then results in five quantitative values, one for each importance oriented section implementation grade. Following the evaluation process, these values are used for the determination of the quantitative values of the security level of each control area *C*. It follows the steps fuzzification, inference, and defuzzification.

During the fuzzification, the quantitative values of the importance oriented section implementation grades are linked to relating fuzzy set functions for implementation grades due to algorithmic reasons. Analogue, fuzzy set functions for output data are defined. During the inference, a set of rules which explicitly considers the individual importance of a section transfers differently combined input data (for grades A to E) to one output each. On the bases of firing rules, the inference leads to the containment of the relevance area of the fuzzy output functions. In the next step, defuzzification supports to extract a quantitative value out of the relevance area. In this context, the barycentric method is used to harmonize the domain between the function of the lowest up to the function of the highest possible output as well as it is used to address the final quantitative security level value on the bases of the harmonized domain in combination with the contained area of relevance. Thereby, the γ-operator is used in the aggregation process for the weighting of sections [Zi01] in order to recognize the weakest links adequately.

For OCI, a technical implementation of ECI supports to automatically apply an otherwise time consuming calculation as well as the technological support enables to transparently visualize evaluation results [KSST07]. As result, a realized optimization process can rank the measures necessary and leading to a strong enhancement of security down to rounding off ones so that limited resources can be invested targeted.

2.6 Integrated program management

Four layers have been presented so far each containing methods to handle the specific STO challenges of information security management each with a strong economic focus. As linking element, an integrated program management that supports annual planning including Resource Management and the definition of the key performance indicators is defined. It stretches over the whole BORIS pyramid and summarizes all initiatives, projects and services under one umbrella aiming to guarantee a transparent overview over the security infrastructure landscape, to minimize project redundancies, to install a proper prioritization process and to directly derive thorough resource management duties [KSST07].

So, program management in this case is more than only about managing programs. It is also about providing services for managing the continuing and ongoing activities and about the alignment of these activities to the overall enterprise goals. Thereby, it follows a systematic called PDCA (Plan-Do-Check-Act) that especially achieved attention with the work of *Deming* [De00] and is also part of security management standards [ISO05a; ISO05b; Ny05]. For the BORIS needs, this process was slightly modified in order to better handle the specific challenges of the introduced methods in a holistic and integrated manner what by no means represents a departure from the fundament of the PDCA principle. The adopted process is defined as:

1. Transferring strategic and compliance driver top-down to information security objectives and defining the business security performance measurement system
2. Deriving and defining acceptable risk levels and comparing actual and debit state in order to extract information about the adequacy of objectives and measures
3. Optimizing the information security infrastructure and linking planning activities to financial tactical methods in order to strongly follow economic principles
4. Analyzing the operational level of the information security infrastructure in order to extract detailed information about optimization potentials
5. Executing new measures and linking the measures characteristics bottom-up to the tactical, the tactical again to the strategic performance measurement level

Whereas the four layers address methods for the vertical supply chain of a business oriented information security management, the program management cycle rounds the framework of by establishing the necessary systematic and closed control loop.

3 Evaluation

Regarding the defined goals at the beginning of this paper, BORIS can fulfill all of them. As layer one holds a system for aligning business to security objectives, R1 is fulfilled. Additionally, a performance scorecard system is outlined that enables to visualize information security performance on a high level of aggregation in different but linked dimensions. The system strongly focuses on business management interests and fulfills R2 in the consequence. Thereby, a balanced set of quantitative as well as qualitative metrics support in visualizing financial, customer, process, organizational, infrastructural and future aspects what ensures a holistic view on the performance influencers and their causes and effects, even if they are not quantitative measurable.

On the tactical layer, PRONOE is introduced to handle risk-investment oriented challenges. It holds a scorecard for assessing enterprises' risk areas and supports in visualizing actual and debit state comparisons what collectively fulfills R3. Because the process tactical methods are directly linked to the financial tactical ones, R4 can be fulfilled. Thereby, PRONOE has several degrees of freedom which make it highly adjustable to individual circumstances which concern for instance:

- The weighting of each risk aspect
- The interdependent weighting of risk aspects
- The aggregation criteria for the management summary

As described before, PRONOE is currently implemented on the bases of the FIRM dimensions. It is running in a real-time environment of an enterprise with world-wide presence, leading their industry [KSST07]. Fig. 5 shows an example of this implementation for the qualitative comparison of actual and debit states in regard to the FIRM dimensions. Thereby, the dimensions are even weighted. The green line indicates the management objectives, the red one the assessment results. If the green one is closer to the centre, the objectives are fulfilled and no action is required, otherwise, initiatives have to be initiated to close the gaps between both lines.

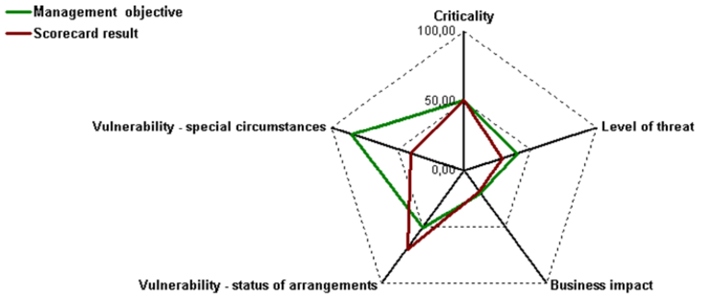


Fig. 5. PRONOE: Example of qualitative results

The quantitative results, where the actual investments per dimension are compared with the targeted volumes, are visualized in the same structure than the qualitative ones as shown in Fig. 5.

It is stressed that the structure of the implementation can of course influence the numerical results. However, this is neither the case for the defined process nor for the interpretation of results for what reason it is implemented and ongoing running in an real and active information security management system.

If gaps are identified, the CB-Toolbox of the BORIS framework offers CoBS or ROSI calculations for dealing with investment decisions on project level. To support this process, BORIS contains the ECI and OCI methods for explicitly addressing the areas of action from the bottom-up perspective.

While ECI uses the Fuzzy-Sets-Theory in order to extract hard data out of fuzzy input, specific quantitative results can be calculated. Additionally, the ECI method can be used as conceptual bases for a technology supported optimization process (OCI) what together fulfills R5. The program management cycle is added in order to link the layers in a planned and systematic matter, what fulfills R6.

The structure of the framework is evaluated by interviewing several information security professionals as well as most parts are already implemented and tested in real industrial environments.

4 Conclusion and outlook

The paper introduced BORIS, a framework for information security management which consists of four layers connected with a program management cycle in order to ensure a closed control loop. Each layer holds methods to deal with strategic, tactical or operational challenges of the topic of interest.

In comparison to currently existing information security management frameworks, the main and innovative advantage of the BORIS framework is that it strictly ensures business orientation in the entire process of information security management. The defined methods follow systematically the chain from business goals, including compliance requirements, to information security measures. Qualitative and quantitative metrics as well as instruments to deal with financial concerns are offered what stresses the character of the framework of being a concept for business oriented management.

Although the contribution presents a systematic and holistic concept, the authors point out that ongoing work has to be done. For example, the system for transferring business goals to security goals has to be enhanced. In this context, the authors currently examine the opportunity to directly link the strategic information security scorecard dimensions and objectives to an enterprise balanced scorecard. Furthermore, it should be analyzed which system is the most suitable one to constitute the bases for the risk assessment process.

Nevertheless, the authors believe that the already presented, current version of BORIS enables enterprises and its information security management to overcome several difficulties in the daily life of security management. It helps to get a transparent insight into the gaps to identify not only what to do but what to do aligned to business goals and financial balance.

References

[AM06] Anderson, Ross; Moore, Tyler: The Economics of Information Security. In: Science, Vol. 314, No. 5799. (2006) 610-613

[Ba01] Baschin, Anja: Die Balanced Scorecard für Ihren Informationstechnologie-Bereich. Ein Leitfaden für Aufbau und Einführung. Frankfurt/Main (2001)

[BMR00] Biethahn, Jörg, Mucksch, Harry; Ruf, Walter: Ganzheitliches Informationsmanagement. Band I: Grundlagen, 5., unwes. veränd. Auflage. München/Wien (2000)

[BSI05] BSI: IT Basic Protection Catalogues, German Federal Office for Information Security (BSI), http://www.bsi.de/english/publications/bsi_standards/ index.htm (2005)

[Ca04] Cavusoglu, Huseyin: Economics of IT-Security Management. In: Camp, Jean L.; Lewis, Stephen (Ed.): Economics of Information Security. Boston et al. (2004) 71-83

[CCR04] Cavusoglu, Hasan; Cavusoglu, Huseyin; Raghunathan, Srinivasan:: Economics of IT Security Management: Four Improvements to current Security Practices. In: Communications of AIS, Vol. 2004, No. 14. (2004) 65-75

[CW04] Camp, Jean L.; Wolfram, Catherine: Pricing Security. In: Camp, Jean L.; Lewis, Stephen (Ed.): Economics of Information Security. Boston/Dordrecht/London (2004) 17-34

[De00] Deming, W. Edwards: Out of the Crisis. Cambridge, Mass. (2000)

[GB02] Gabriel, Roland; Beier, Dirk: Informationsmanagement. Band 3: Spezialthemen des Informationsmanagements. Lehrmaterialien im Studienfach Wirtschaftsinformatik 36/02, Lehrstuhl für Wirtschaftsinformatik, Ruhr-Universität Bochum, Bochum (2002)

[GB03] Gabriel, Roland, Beier, Dirk: Informationsmanagement in Organisationen. Stuttgart (2003)

[GL02] Gordon, Lawrence A.; Loeb, Martin P.: Return On Information Security Investments: Myths vs Realities. In: Strategic Finance, Vol. 84, No. 5. (2002) 26-31

[GL04] Gordon, Lawrence A., Loeb, Martin P.: The Economics of Information Security Investment. In: Camp, Jean L.; Lewis, Stephen (Ed.): Economics of Information Security. Boston/Dordrecht/London (2004) 105-127

[GSW08] Gabriel, Roland; Sowa, Sebastian; Wiedemann, Jochen: Improving information security compliance – A process-oriented approach for managing organizational change. In: Proceedings of the Multikonferenz Wirtschaftsinformatik 2008 (MKWI 2008), Munich (2008)

[Fi05] Fitzgerald, Todd. (2005): Building Management Commitment through Security Councils, in: Information Systems Security, Vol. 14, No. 2. (2005) 27-36

[SCC07] Supply Chain Consortium: Benchmarking Do's and Don'ts. In: Industry Week/IW, Vol. 256, No. 12 (2007) 50-50

[ISF08] Information Security Forum, Fundamental Information Risk Management (FIRM), http://www.securityforum.org/ (member access only) (2008)

[ISO05a] International Organization for Standardization, ISO/IEC 17799:2005 "Information technology - Code of practice for information security management"

[ISO05b] International Organization for Standardization, ISO/IEC 27001:2005, "Information technology - Security techniques - Information security management systems – Requirements"

[ITGI07] ITGI: CObIT 4.1, Framework, Control Objectives, Management Guidelines, Maturity Model, IT Governance Institute, Rolling Meadows (2007)

[KL07] Klempt, Philipp: Effiziente Reduktion von IT-Risiken im Rahmen des Risikomanagementprozesses, Bochum, Univ., Diss. (2007)

[KN96] Kaplan, Robert S., Norton, David P.: Using the Balanced Scorecard as a Strategic Management System. In: Harvard Business Review, Vol. 74, No. 1 (1996) 75-85

[KN05] Kaplan, Robert S., Norton, David P.: The Balanced Scorecard: Measures That Drive Performance. In: Harvard Business Review, Vol. 83, No. 7/8 (2005) 172-180

[KSST07] Klempt, Philipp; Schmidpeter, Hannes; Sowa, Sebastian; Tsinas, Lampros: Business Oriented Information Security Management – A Layered Approach. In: Proceedings of the 2nd International Symposium on Information Security (IS'07), Vilamoura (2007) 1835-1852

[La05] Lange, Jörg A.: Sicherheit und Datenschutz als notwendige Eigenschaften von computergestützten Informationssystemen. Ein integrierender Gestaltungsansatz für vertrauenswürdige computergestützte Informationssysteme, 1. Auflage. Wiesbaden (2005)

[La06] Lapide, Larry: Questions to Ask when Reviewing the Benchmarking Data. In: Journal of Business Forecasting, Vol. 25, No. 4 (2007) 4-7

[La07] Lardschneider, Michael: Security Awareness – Grundlage aller Sicherheitsinvestitionen. In: DuD, Datenschutz und Datensicherheit, 31. Jg., Nr. 7. (2007) 492-497

[La95] Laprie, Jean-Claude: Dependability of Computer Systems: from Concepts to Limits. In: Proceedings of the Sixth International Symposium on Software Reliability Engineering. (1995) 2-11

[Lo04] Loomans, Dirk C.: Information Risk Scorecard macht Sicherheitskosten transparent. In: Mörike, M. (eds.): HMD 236 “Praxis der Wirschaftsinformatik - IT-Sicherheit” (2004)

[Ny05] Nyanchama, Matunda: Enterprise Vulnerability Management and Its Role in Information Security Management. In: Information Systems Security, Vol. 14, No. 3 (2005) 29-56

[Pe05] Peltier, Thomas R.: Implementing an Information Security Awareness Program. In: Information Systems Security, Vol. 14, No. 2 (2005) 37-48

[Po07] Powell, Robert: The Boom in Benchmarking Studies. In: Journal of Financial Planning, Vol. 20, No. 7 (2007) 5-23

[SCL05] Sherwood, John; Clark, Aandrew; Lynas, David: Enterprise Security Architecture, A Business Driven Approach (2005)

[So02] Soo Hoo, Kevin J.: How Much Is Enough? A Risk Management Approach to Computer Security. Workshop on Economics and Information Security, University of California. Berkeley, CA (2002)

[Sc06] Schneier, Bruce: Beyond Fear, Thinking Sensibly About Security in an Uncertain World. New York (2006)

[Ti03] Tiller, Jim: The Business of Security. In: Information Systems Security, Vol. 12, No. 5 (2003) 2-4

[Ts07] Tsinas, Lampros: PRONOE, Process and Risk Oriented Numerical Outgoings Estimation – Vorschlag für eine Methodik zur risikoorientierten Kosten-Nutzen-Balance im Informations-Sicherheits-Management. In: KES, Zeitschrift für Informations-Sicherheit, 23. Jg., Nr. 4. (2007) 44-49

[WK05] Werners, Brigitte; Klempt, Philipp: Verfahren zur Evaluation der IT-Sicherheit eines Unternehmens, Arbeitsbericht Nr. 12, Institut für Sicherheit im E-Business (ISEB), Bochum (2005)

[WFCR01] Wei, Huaqiang; Frinke, Deb; Carter, Olivia; Ritter, Chris: Cost-Benefit Analysis for Network Intrusion Detection Systems. CSI 28th Annual Computer Security Conference, October 29-31, 2001, Washington, D.C. (2001), http://www.csds.uidaho.edu/deb/costbenefit.pdf

[Xe87] Xerox Corporation: Leadership through quality: Implementing competitive benchmarking (1987)

[Zi93] Zimmermann, Hans-Jürgen: Fuzzy Technologien: Prinzipien, Werkzeuge, Potentiale. Düsseldorf (1993)

[Zi01] Zimmermann, Hans-Jürgen: Fuzzy set theorie – and its applications. 4th ed., Boston et al. (2001)