2009

INTEGRATED INFORMATION SECURITY RISK MANAGEMENT – MERGING BUSINESS AND PROCESS FOCUSED APPROACHES

Sebastian Sowa
Ruhr-University of Bochum, Institute for E-Business Security (ISEB)

Lampros Tsinas
Munich Re, Koeniginstr

Hanno Lenz
ERGO Insurance Group

Roland Gabriel
Ruhr-University of Bochum, Chair of Business Informatics

INTEGRATED INFORMATION SECURITY RISK MANAGEMENT – MERGING BUSINESS AND PROCESS FOCUSED APPROACHES

Sebastian Sowa[1], Lampros Tsinas[2],
Hanno Lenz[3], Roland Gabriel[4]

Abstract

Previous papers mostly dealt with specific views of information security management (either technical, organizational for instance). Recently, major progress has been achieved in the development of a business driven approach with BORIS (Business Oriented management of Information Security) and a process-oriented approach called ORBIT (Operational Risks in Business and IT). An integrated framework is being described in this paper that bases on the beneficial and complementary merge of both approaches. It supports management of an enterprise's information security functions with a strong economic focus whereby it specifically links business and information security objectives. The methodology to be presented has proven to be reliable, user friendly, consistent and precise under real conditions over several years in enterprises with world wide presence.

1. Introduction

1.1. Situation

Several models, methods and measures were introduced in the past each covering particular aspects of Information Security (IS) or information risk management. Most of the approaches focus primarily on technical issues but recently, also business oriented approaches for managing IS can be identified in the literacy (i.e. [1], [16]). But again, many of the approaches mainly focus on specialized fields without meeting the challenges of a holistically integrated and practicable concept. They lack in integrating the different interests of relevant actors and even more important, they lack in establishing a system that transparently links business with IS objectives and measures as well as these objectives and measures with a method for defining optimal investment policies. To handle these challenges, a framework for managing IS with a strong economic focus is presented in the following. This starts with the clarification of the appreciation of used terms and intended goals.

[1] Ruhr-University of Bochum, Institute for E-Business Security (ISEB), GC 3/29, 44780 Bochum, Germany

[2] Munich Re, Koeniginstr. 107, 80802 Munich, Germany

[3] ERGO Insurance Group, Victoriaplatz 2, 40477 Düsseldorf, Germany

[4] Ruhr-University of Bochum, Chair of Business Informatics, GC 3/132, 44780 Bochum, Germany

1.2. Terms

Information in this paper is defined as an explanatory, significant assertion that is part of the overall knowledge as well as it is can be seen as specific, from human beings interpreted technical or non-technical processed data [7]. This definition is precisely in line with the ISO/IEC standards which state 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" [9].

As consequence of the appreciation of information, IS has to cover technical as well as non-technical topics. In this context, the ISO/IEC declares that whatever "form the information takes, or means by which it is shared or stored, it should always be appropriately protected. IS 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" [9].

1.3. Goals

The goals defined in this paper are in line with findings in several topic-near publications like [5] and [6], added with the result of several discussions to scientist, practitioners, and of reviews of content related papers [17].

R1: As IS is seen as business and strategic management topic, the Information Security Management (ISM) framework then has to enable executives to transparently link business to IS objectives.
R2: The framework should support to answer questions about IS performance as well as it should support to address areas suitable or necessary to improve the performance influencing indicators.
R3: The process of defining concrete and measurable indicators for the security target as well as for the current state in different levels of detail should be supported.
R4: To close identified gaps, especially investment decisions have to be addressed in the context of the regarded business oriented management framework. Thereby, executives should be given support for the processes of finding and defining cost benefit balanced investment strategies.
R5: When measures are running, the framework should offer a method for evaluation that can also be used for optimizing the economic and strategic performance of the overall IS infrastructure.
R6: The methods defined have to be integrated into a management process that enables the continuously and especially sustainable business oriented ISM.

To fulfil the requirements respectively to reach the goals, the present paper presents two already existing components, BORIS (Business Oriented management of Information Security) and ORBIT (Operational Risks in Business and IT), as well as it introduces the reader to a data model for the coexistence of the currently singularly successfully existent concepts in real environments.

2. BORIS Design

2.1. Overview

To handle especially business oriented ISM issues, a framework for the Business Oriented management of Information Security (BORIS) was introduced by [17]. As seen in Figure 1, the framework consists of four layers whereby each layer covers particular aspects of strategic, tactical and operational ISM challenges.

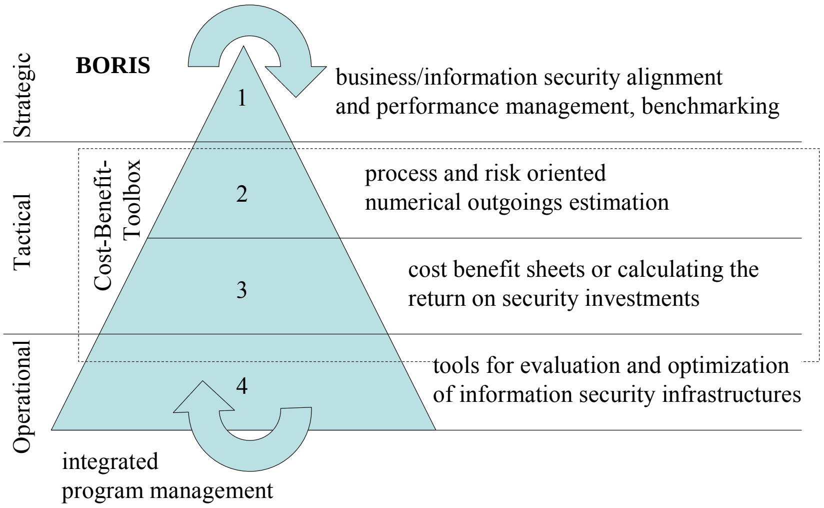
Strategic
BORIS
1
business/information security alignment
and performance management, benchmarking
Tactical
Cost-Benefit-
Toolbox
2
process and risk oriented
numerical outgoings estimation
3
cost benefit sheets or calculating the
return on security investments
Operational
4
tools for evaluation and optimization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

Figure 1: BORIS general topology

The top level focuses on the business and ISM interaction, the second and third layers deal with linking the results of the strategic methods to specific IS objectives and with defining a balanced investment policy for implementing and managing measures targeted to close identified gaps. The fourth layer holds tools for the evaluation and optimization of IS infrastructures while an integrated program management rounds the framework of to ensure continuous effort of the tasks of interest. As the framework is presented in detail in [17], the current paragraphs have the goal of briefly recapitulating major findings and benefits.

2.2. Business Strategic Methods

The top layer of BORIS deals with Business/Information Security Alignment and Performance management (BISAP). It consists of a transferring system for linking strategic as well as legal, regulatory, standard implied and contractual drivers to IS objectives and a scorecard system with which performance is measured. Here, the theoretical basis is laid by the Balanced Scorecard [10] that is widely accepted and adopted for several branches and industries as well as the general idea is used for years in the context of information management for instance (i.e. [7]).

Because of the aim of connecting the BORIS system with an enterprise Balanced Scorecard, the business strategic method defined here integrates IS performance objectives and metrics in the traditional dimensions finance, customer, processes and future. An organizational dimension is added to the system to match with the requirements of several standards which accentuate the importance of organizational IS performance as well as a sixth dimension is added which covers the importance of the technological IS infrastructure. Analogue to the traditional Balanced Scorecard, also the dimensions of BISAP are connected through a knowledge-based steering methodology.

The legal, regulatory, standard implied and contractual as well as 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 officers in charge of legal affairs for instance have to cooperatively agree to. Transferring tables thereby are offered to support this process: Business requirements (formulated in “business language”) here are linked to IS 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.

Benchmarking replenishes BISAP. As widely used and accepted method [14] it is anchored in BORIS to supports to identify the own level of maturity while the individual records of performance are set in relation to a peer group of interest. This offers to benefit from the results if data is correctly interpreted and the peers are of adequate competitive importance [13]. For BORIS, the Information Security Status Survey provided by the Information Security Forum (ISF) is currently used. To transfer benchmarking results in the next step 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 BISAP method are linked to process tactical methods.

2.3. Process Tactical Methods

The Process and Risk Oriented Numerical Outgoings Estimation (PRONOE) method is introduced in detail by *Tsinas* [18]. It is directly linked to BISAP as it uses its output as operational guideline while the data processed in PRONOE again is delivered up to layer 1 in an aggregated format. PRONOE contains three components [17]: A risk assessment layer for determining the qualitative actual and debit, the (100- X)% rule for determining the quantitative debit and a process for the cost-benefit balancing comparison of the qualitative and quantitative actual and debit values which especially supports to address financial investment policy goals.

Thereby, a management committee , consisting of the persons in charge of business management, should determine the objectives what concretely means to agree on a specific level of acceptable risk exposure and on the areas which require additional risk controls. This gives the qualitative debit. The qualitative actual then is assessed using common risk assessment methods like scorecards for instance. For BORIS, a questionnaire offered by the ISF is used to address the status of the risk areas in currently five dimensions [8]: Criticality, Level of threat, Business impact, Vulnerability – status of arrangements, and Vulnerability – special circumstances. Recently, effort is spending to transform this layer from the proprietary ISF scorecard to an ISO 27001 aligned structure. This would allow everybody to use this model, and certainly it would support the ISO dimension with eleven risk areas.

The (100- X)% rule transfers the level of acceptable risk to protection areas, defined as 100 percent minus the accepted level of risk in percentage. It bases on the assumption that each assertion about acceptable risks directly implicates that any further risks are not accepted and that each assertion also defines the investment areas necessary to reduce the overlapping risk levels to acceptable ones.

For cost-benefit balancing comparisons, the actual investment situation is assessed and set in relation to the debits calculated by using the (100-x)% rule. As information is generated here about whether the established security level could have been realized using defined resources or whether an objective has been left unmet because sufficient resources were not available, this element of PRONOE supports to address the appropriateness of the IS investments [12].

2.4. Financial Tactical Methods

Whenever measures have to be implemented in order to reduce defined overlapping risk levels, questions about investments on a more detailed level arise. Here, BORIS offers the calculation of the Return on Security Investment (RoSI) when accurate data is available. If accurate data is missing, is not existing or statistically significant, Cost Benefit Sheets (CoBS) as presented by *Sowa et al.* [17] should be used. CoBS are quite similar to the approach of *Schneier* [15] whereby a systematic documentation can enhance CoBS quality as well as it enabled to appropriately justify but also revise investment decision.

2.5. Operational Evaluation and Optimization

So far, strategic, process and financial tactical methods are introduced and linked to each other what demonstrates a closed chain from business to security business management. For rounding of the quantum of methods, the operational level of BORIS holds methods for evaluating the current controls infrastructure (ECI) as well as for optimizing the necessary controls infrastructure (OCI). As a comprehensive method capable to deal with ECI/OCI is presented by *Klempt* [11], and *Klempt et al.* [14], the authors of the current paper abdicate to discuss the method further on. Instead, the method for managing Operational Risks in Business and IT (ORBIT) is introduced in the following paragraphs.

3. ORBIT Design

3.1. Overview

Unlike BORIS, ORBIT is a methodology presented first-time in this paper to the scientific community. Chronologically it was designed well after BORIS was already implemented and a certain level maturity achieved. Thereby, the design of ORBIT benefits of underlying effort in the development of BORIS and completes the missing design elements systematically.

ORBIT is a system aiming to control operational risks in business processes in regard to information technology consisting of elements called Knowledge Cells (KCs). KCs can be understood as data container that incorporate diverse kinds of topic related information and associations that are of specific interest for a targeted group of information consumer [2], [3]. The system bases on the assumptions that information risks are the primary ones of concern and that technology itself in the consequence has no own risks – apart from internal dependencies towards itself (recursion). Additionally, it is assumed that the requirements of the essential security objectives – availability, integrity, confidentiality and authenticity – are defined within the business processes. From background of this, the following KCs lay the foundation of the approach presented here: Business process, IT system, application system, threat, risk, and measure. In general, the model could be extended to meet the requirements of any kind of operational risks. However, this is not the subject of the paper presented.

The KC business process contains the descriptions of an enterprise's core processes, especially in regard to the four typical IS objectives while the KC IT system holds information about the enterprises' essential IT systems and networks. In addition to general information, the description here also includes the currently achieved degree of performance in regard to the IS objectives of interest, for example, the current confidentiality level or availability class. An IT system thereby may be a platform that supports 1…n business processes. It directly serves as a support for the business process and is described in its own KC. Kinds of threats are also described in a separate KC whereby a threat is defined as one possible scenario or a threatening potential that could impact IT systems [4].

Closely related with threats, the KC risk holds information derived from the quantification of possible threat impacts, whereby common methods like multiplying a probability of occurrence with possible impacts are being used. Finally, the KC measure contains possible actions to achieve IS objectives. As seen in Figure 2, the KCs are linked to each other whereby attributed associations are being used.

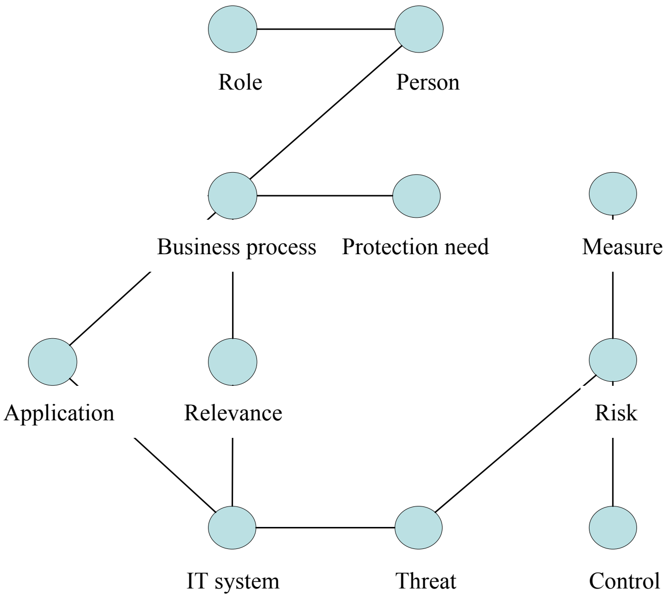

Figure 2: ORBIT – Typology

3.2. Method

The systemic approach for visualizing the essential IT risks in regard to the core business activities of an enterprise implies to logically link the relevant KCs. Thereby, business processes, IT systems and risks are of essential importance for what reason their relations and the main connected KCs up to measures as seen in Figure 3 are being discussed in more detail in the following.

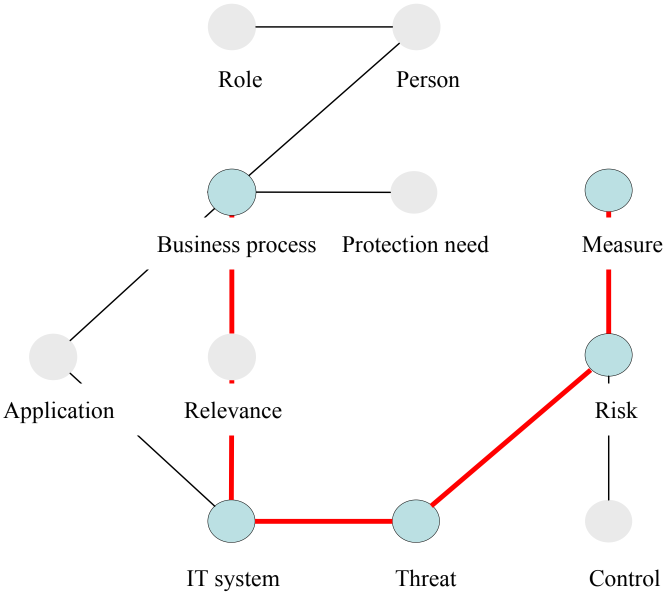

Figure 3: ORBIT – Essential KCs

Business process – IT system: This link enables the identification of dependencies of business processes and IT systems. Here, the targeted level, e.g. the required level of availability of an IT system for a business process, can be compared to the current condition. Thereby, a requirement is fulfilled if all systems comply with the requirements of the particular business process while a requirement is not fulfilled if one or more IT systems deviate from target conditions towards unstable ones. A requirement is surpassed if all IT systems do not undercut the target condition and single ones even hold a higher security level. A comparison of target and current conditions allows a dedicated assessment of necessary measures on the basis of direct dependencies between business processes and IT systems.

IT system – Threat: Standardized threat catalogs support in defining individual threat scenarios for an enterprise's IT. Thereby, a scenario can be relevant for 1...n IT systems whereby mainly threats are regarded that may lead to hostile risks when quantifying. Therefore, the reference of a risk and a business process can be created after the quantification of the threat. In the context of vulnerability assessments, threats are being analyzed that jeopardize the proper operation of IT components and can therefore lead to noncompliant security objectives. A differentiation of threats, e.g. with regard to location and type of interface, has to be carried out.

Threat – Risk: Threat scenarios that affect single or accumulations of IT systems here are carried over to quantifications. A quantification is the classification of a threat in regard to its probability of occurrence and impact. The levels of probability range from almost impossible to very certain, effects are classified by using a range of insignificant up to hostile. Intrinsic connections allow risks to be allocated to business processes through the relation of threats towards the IT systems.

Risk – Measure: For the purpose of risk controllability, risk measures (i.e. controls) have to be implied that observe at least one risk component (the probability of occurrence or the impact) as well as they should reduce the individual classified value. Here, a decision to take a risk and, at the same time, keep a corresponding amount of capital as a reserve, is also to be considered as a IS measure. This special measure is then employed when the investment of the IS measure is higher than the amount of loss, quantified by the department. The quantification of threats finally leads to a survey of risks that have to be controlled as shown in Figure 4.

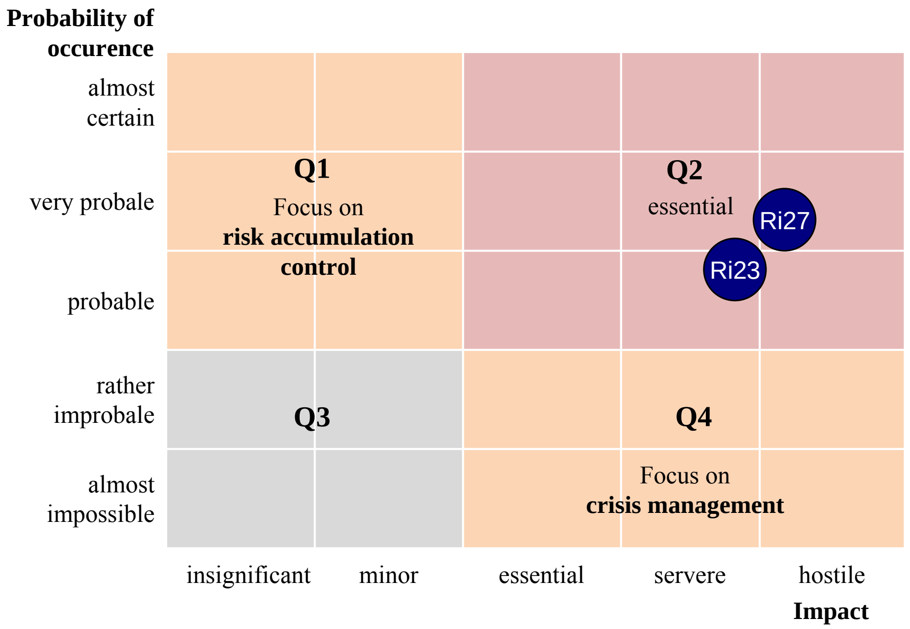

Figure 4: ORBIT – Risk matrix

The risk matrix is separated into four parts – following industry best practices. In quadrant Q1, the focus lays on the control of accumulated risks. Here, it is analyzed if the risk also occurs in other sectors of business and if there are any correlations with other risks for instance. Shifting to Q2, the criticalities of risks like those of Ri23 and Ri27 are of such height that they need constant observation. Risks that are categorized in Q3 should undergo yearly evaluation. In Q4, the main focus is laid on crisis management. Enterprises should be prepared for worst-case scenarios here for instance.

At the point of the risk assessment, the level of threat is defined considering all measures set up for risk control in this context. This so called net risk method is used as a hypothetical assignment of threat levels under the theoretical assumption that no minimizing measures were implemented (gross risk method) is not convenient as it doesn't reflect the de facto situation. As far as further measures in regard to the net risks have to be planned, the corresponding risk can be evaluated at the next interval under consideration of the degree of implementation. The authors accentuate thereby that the implementation of a regular reassessment process has to be anchored in this management system – starting to run after the implementation of relevant measures at the latest.

4. Merging the Approaches: A generic Data Model for the Integrated Information Security Risk Management

After introducing BORIS and ORBIT, the current chapter intends to present a generic data model that bases on the merge of BORIS and ORBIT resulting in a powerful and practicable framework for the business and process focused information security risk management. This data model relies on the fact, that no matter what the management methodology finally is, at the end of the day, the person in charge for the information security risk management functions has to deal with certain key questions like budget, staff, services, strategy, skills, and certainly controls management (e.g. selection and application of proper measurements for the minimization of the information security risks). Thus, this person needs tools capable to support him in answering these questions.

Starting to compare BORIS and ORBIT, one of the first results is that both models have a common nominator: The "control management". No matter, where the need for the selection of a control (i.e. implementation of SPAM-filter, or a security awareness programs for instance) is driven from, it is finally based on a scorecard evaluation of security respectively risk drivers as well as on an appropriate analysis of the cost-benefit situation in this context. An integrated database which contains comprehensively the results of the scorecard evaluations (either from BORIS or/and ORBIT) then is leading to a selection of a control for the driver (a policy or risk for instance) identified. Thereby, to strongly base controls management here on business and economic principles, only those controls will be implemented, which have passed the cost-benefit analysis successfully. Otherwise, because it might become traceable that some of the controls might cause higher investment than the expected benefit, they'll be rejected.

Thus, the role of ISM executives (i.e. CISO or CSO) can be supported in regard to decisions about the adequate control selection as well as it can enhance the productivity of the implemented controls while at the same time the efficiency can be increased. Nonetheless, ISM will still have to deal with decisions and management regarding the budget, skills, strategy, service and people in the IS organization which are not focused on in this paper. Realistically and based on the actual experience of the authors, the merge of BORIS and ORBIT as visualized through Figure 5 is highly enticing and promising to become a leading edge method for information security risk management.

Regarding the defined goals at the beginning of this paper, the presented framework can fulfil all of them. As BORIS layer one holds a system for aligning business to security objectives supported by the linkage of the KCs business processes up to risks, R1 is fulfilled. As the scorecard system outlined in the BORIS concept enables to visualize IS performance on a high level of aggregation, R2 is reached in the consequence.

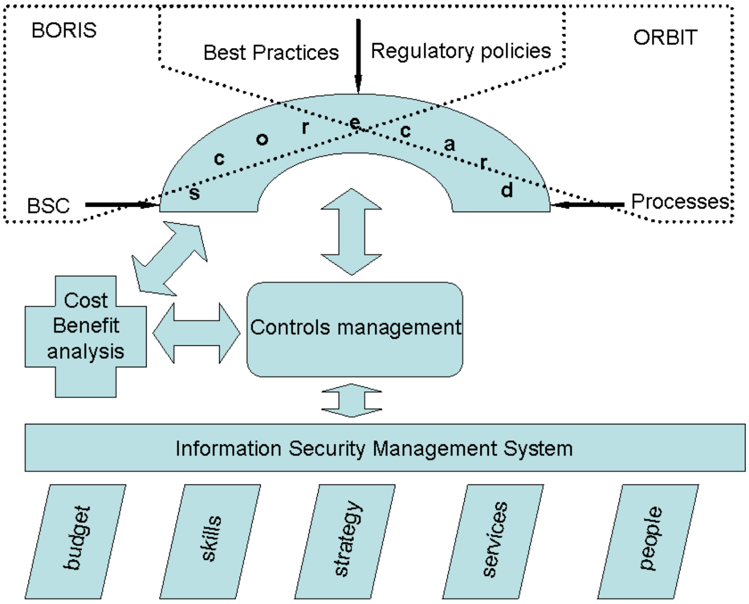

Figure 5: Integrated Information Security Risk Management

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. Alternatively, ORBIT can be used in this context what collectively fulfils goal R3. Because both models are directly linked to the cost-benefit-toolbox of BORIS that is formed by its layers 2 and 3, offering support for dealing with concrete investment decisions, R4 is reached. Thereby, PRONOE offers the opportunity of calibrating different screws in regard to the individual denotation of a risk area, in regard to the interdependencies of risks as well as in regard to the aggregation criteria for the management summary [17]. In addition to the cost-benefit-toolbox, the ECI and OCI methods help in identifying areas of necessary action from the bottom-up perspective what enables to reach goal R5. A program management cycle that can be overlapping BORIS, including the ORBIT world, is rounding off the framwork in order to link the different tools in a planned and systematic matter, finally fulfilling R6. The structure of the framework is evaluated by interviewing several scientists and IS professionals as well as most parts of BORIS as well as ORBIT in its full structure are already implemented and running successfully in real-time environments of enterprises with world-wide presence.

5. Conclusion and Outlook

The paper introduces a comprehensive model for the integrated security risk management, which is vital for any public or private organization. The higher the degree of implementation of the presented model, the higher is the expectation to see optimization of expenses on the one (i.e. minimization) and of the efficiency on the other hand (i.e. maximization of the effectiveness). The authors strongly believe that it is a matter of time where methodologies like the described ones will dominate the behaviour of IS professionals. The main reason for this assumption is, BORIS and ORBIT as well as the introduced common framework "speak" the same language at the control level.

Although the paper presents a systematic and holistic concept, ongoing work has to be done. For instance, BORIS and ORBIT are productively used in industrial environments solitary but their integration is just on the design stage. Here, a detailed data-model has to be developed and furthermore used for the development of the database what is one of the most challenging but beneficial tasks. Indeed, the authors predict to have the integrated method fully supported by a combined tool soon to be finalized. Tremendous effort has to be spend to have this vision realized, and the effort itself has to be a subject of decision making and furthermore to show the positive economic impact, as any other "security control". In other respects, any further work in this direction will become obsolete – which is not going to be the case, as the author experienced so far. Nevertheless, the authors believe that the current versions of BORIS and ORBIT already enable enterprises to overcome several difficulties in the daily life of ISM. 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.

6. References

[1] ANDERSON, R.; MOORE, T., The Economics of Information Security, in: Science, Vol. 314, No. 5799 (2006).

[2] BAGNARA, S., Towards Telework in Call Centres, Euro-Telework Project Report, November 2000.

[3] BARBERÁ TOMÁS, D.; DE LOS REYES LÓPEZ, E.; PAGE DEL POZO, Á; LACUESTA, J. S., 'Contextualized knowledge'. Insights from the Organizational Memory of a Research Institute, Triple Helix 5, The Capitalization of Knowledge: cognitive, economic, social & cultural aspects, Center, Turin, Italy, 18.-21.05.2005.

[4] BSI, Standard 100-1, Information Security Management System (ISMS), Version 1.0, Federal Office for Information Security (BSI), Bonn 2005.

[5] CAVUSOGLU, H., Economics of IT-Security Management, in: J. L. Camp; S. Lewis (Ed.), Economics of Information Security, Boston et al. 2004.

[6] CAVUSOGLU, H.; CAVUSOGLU, H.; RAGHUNATHAN, S., Economics of IT Security Management: Four Improvements to current Security Practices, in: Communications of AIS, Vol. 2004, No. 14 (2004).

[7] GABRIEL, R., BEIER, D., Informationsmanagement in Organisationen, Stuttgart 2003.

[8] INFORMATION SECURITY FORUM, Fundamental Information Risk Management (FIRM), 2008.

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27001:2005: Information technology - Security techniques - Information security management systems – Requirements, Geneva 2005.

[10] KAPLAN, R. S., NORTON, D. P., Using the Balanced Scorecard as a Strategic Management System, in: Harvard Business Review, Vol. 74, No. 1 (1996).

[11] KLEMPT, P., Effiziente Reduktion von IT-Risiken im Rahmen des Risikomanagementprozesses, Bochum 2007.

[12] KLEMPT, P.; SCHMIDPETER, H.; SOWA, S.; TSINAS, L., Business Oriented Information Security Management – A Layered Approach, in: R. Meersman; Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Berlin et al. 2007.

[13] LAPIDE, L., Questions to Ask when Reviewing the Benchmarking Data, in: Journal of Business Forecasting, Vol. 25, No. 4 (2007).

[14] POWELL, R., The Boom in Benchmarking Studies, in: Journal of Financial Planning, Vol. 20, No. 7 (2007).

[15] SCHNEIER, B., Beyond Fear, Thinking Sensibly About Security in an Uncertain World, New York 2006.

[16] SOO HOO, K. J., How Much Is Enough? A Risk Management Approach to Computer Security, Workshop on Economics and Information Security, University of California Berkeley, CA 2002.

[17] SOWA, S.; TSINAS, L.; GABRIEL, R., BORIS – Business ORiented management of Information Security, Workshop on the Economics of Information Security, Dartmouth College, Hanover, NH, 25.-28.06.2008.

[18] TSINAS, L., 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, Vol. 23, No. 4 (2007).