UDC 681.518

H. L. GROB, Prof. Dr., European Research Center for Information Systems, University of Muenster, Muenster, Germany,
grob@ercis.de
G. STRAUCH, European Research Center for Information Systems, University of Muenster, Muenster, Germany,
gereon.strauch@ercis.de
C. BUDDENDICK, Dr., European Research Center for Information Systems, University of Muenster, Muenster, Germany,
christian.buddendick@ercis.de

A PROCEDURE MODEL FOR EVALUATING IT-SECURITY INVESTMENTS

Безпека інформаційних систем у теперішній час є життєво важливим фактором для компаній. Багато різних вимірів, від технічних до організаційних, є доступними для досягнення прийнятного рівня безпеки. У недалекому минулому було розроблено методи підтримки прийняття рішень при оцінюванні прибутковості інвестицій у IT-безпеку. Проте інтегральні процедурні моделі для повного управління IT-безпекою до цього часу не знайдені - ані у літературі, ані на практиці. У цієї статті ми пропонуємо середовище, яке дає можливість аналізувати результати альтернативних інвестицій у безпеку з точки зору, орієнтованої на процеси. Ми здійснили поглиблений аналіз сучасного стану справ у галузях синхронізації IT та бізнесу та управління IT-безпекою з метою ідентифікувати прийнятні концепції для цього середовища. Спеціальну увагу приділено вимогам до IT-безпеки критичних бізнес-процесів.

The security of information systems is a vital factor for companies nowadays. In order to achieve an adequate level of security, a variety of distinct measures is available, ranging from technical measures to organizational measures. In near past suitable methods for decision support especially for the assessment of the profitability of IT-security investments have been developed. But integrated procedure models for a complete it-security controlling can neither be found in literature nor in practice. With this article, we propose a method framework that enables the analysis of the results of alternative security investments from a process-oriented perspective. As a basis, we have conducted an in-deep analysis of the state-of-the-art in the fields of IT-Business-Alignment and IT-security management in order to identify suitable concepts for the framework. A special focus lies on the requirements of IT-security controlling of critical business processes.

1. Introduction. The necessity for a risk management concerning IT-security results exempted from economic considerations just as from different standards and requirements, e.g. such as the Sarbanes Oxley Act [1-4]. An evidence thereof is the in the past above-average increase of IT-security budgets compared to overall IT budgets [5]. Nether less there are just a few findings in this field in terms of decision support by analyzing the profitability of such measures even if necessity is broadly accepted in theory and practice [6]. Most of the existing work can be characterized as vague, unusable or without reference to concrete recommendations for a course of action [7-9].

The measurement of profitability for IT-security measures implies similar challenges as those in the field of IT investments in general. Although the IT productivity paradoxon has been considered as outdated for years [10; 11], recent studies indicate still skepticism of executives whether IT investments can provide an adequate value from a company’s point of view [12; 13]. This problem is even more obvious in the field of IT-security due to the fact that that the effects of successful measures are exclusively indirect, because they contribute to the reduction of (future) risks [14-16]. The statement: "IT-security functions have been valuable whenever nothing has happened.” [6] underlines this problem area. Moreover, it is insufficient to analyze just one measure independent, since there are often interdependencies among various IT-security measures and only a bundle of measures can be accounted for success [17]. Meanwhile this complexity calls for taken a detailed set of different parameters into account, the practical applicability calls for a simple to compute method. This conflict is enforced by the reciprocal expert-layman relations in this field where accounting is conducted by business specialists and implementation and design of measures by technical experts [18]. In particular, it is necessary that all relevant aspects from technical and business point of view are considered when providing a decision recommendation [19]. An analysis of the state-of-the art in the field of IT-security management illustrates that the suggested methods are either theoretically inexact or practically unapt [19; 20]. Traditional approaches do mostly not calculate the corresponding value proportion of these measures. The corresponding return is mandatory for the assessment of efficiency [19-21]. Findings in the field of IT-Business-Alignment offer the opportunity to overcome this shortcomings, because they allow to compute the return by a combination of the business process-view and the IT-process-view [22], it has to be examined whether IT-Business-Alignment approaches, which explicitly consider this relationship, can be adopted for the controlling of IT-security measurements. Most approaches in context suppose a linear exchange relationship between expected loss and the costs of security measures. This procedure does not apply for information systems, which have vital meaning for the organization.

Based on these requirements, we suggest a procedure model which supports the assessment of the profitability of alternative IT-security investments. Essential for the design of the method framework is the observation that the implications of IT investments first of it all can be observed on the process level [23]. One topic is to integrate the methods for calculation of payments and disbursements for all processes which are affected by IT-security measures to a generic procedure model of IT-risk management-Another is to provide decision support for security investments within critical infrastructures and integrate this into an overall IT-risk management procedure. So we define requirements in this context and offer an outlook to an approach for controlling security measures for critical business processes and information infrastructures (such as data centers). We conclude with a brief summary and an outlook on future research opportunities.

2. IT-business alignment as a design principle for the IT Security management

2.1. Content of IT-Business-Alignment. "IT-Business-Alignment" terms the alignment of the IT-strategy and –infrastructure with the business-strategy and –architecture. The goal is a sustainable creation of value for the company [24; 25]. The term "alignment" is used varyingly in literature [26]. In this context the process, which aims at the achievement of the alignment, is meant [26-28]. Synonyms for alignments used in literature are "fit" [29; 30], "harmony" [31], "integration" [32], "linkage" [33]or "synergy"[34]. One main aspect in the alignment of the IT-perspective with the business-perspective is the security of the information systems as a dimension of process quality with the quality dimensions of security like confidentiality, availability and integrity [35]. Out of this, approaches of the IT-Business-alignment are used are often used in the IT-security literature, e.g. through employing a business process orientation [22; 36-39], or, more explicitly, through adopting various techniques of Business Engineering [37]. Linking IT- and Business-perspective is especially demanded when the efficiency of IT-security measurements is calculated [22]. Most approaches just employ pure metrics in the meaning of calculation rules for top key figures – the determination of the corresponding figures is still a non solved problem [20; 21; 40]. In the next section methods, which were explicitly developed for IT-Business-alignment, are examined concerning their fulfillment of the above stated requirements and their contribution to the calculation of the profitability of IT-security measures. Because the design and valuation of process are of great importance to IT-Business-alignment [41; 42], it has to be checked, in how far decision support methods in the context of business process management and controlling exist and in how far these methods can be employed in alignment-projects.

2.2. Decision support with process models. In earlier publications many decision support methods for IT-Business-alignment can be found. A growing importance to a successful IT-Business-alignment is assigned to process models [26; 43], especially for approaches in the IT-security management context. In the latter the main process-oriented approaches out of literature will be examined concerning their applicability towards the calculation of economic efficiency of IT-security measures. For this the process models have to be extended with further information. This should be information about costs, time and capacities. After this they can be utilized as a basis for process-controlling [19; 44; 45]. Out of the controlling domain several approaches targeting at process-controlling exist. These are for example approaches, where the process performance is evaluated through key figures out of a number of dimensions [46-48]. To be able to state the economic efficiency of the model, multidimensional performance measurement [49] is not suitable. Regarding the transparency of value creation, decision support methods, which provide information about costs or out payments, are needed. To calculate the costs based on process models, activity based costing (ABC) can be employed [44; 50; 51]. Time related information about costs are of great importance for short-term decisions. Because IT-Business-alignment decisions are long-term decisions, cost-oriented approaches are not suitable. Instead of this, in- and out payments should be used for evaluating alternative forms of IT-Business-alignment. Grob & vom Brocke developed an approach to evaluate payments based on process models [52]. The main principle of the method is, that the execution of single functions of a process is connected to long-term monetary consequences. Those are consolidated into one financial key figure [52]. One challenge in the consolidation of these single payments to one series of payments comes up, when the EPC has cycles. With the help of statistical procedures the payments can be aggregated corresponding to the process. This aggregation results in a series of payments which consolidates all original payments of the process. This series of payments serves as the interface to the calculation of financial key figures in a finance plan instrument called Visualization of Financial Implications (VOFI) as an instrument of the dynamic investment controlling [53; 54]. With its help all in- and out payments and the original amount of financial resources corresponding to the project are captured and reckoned up. The results of a VOFI can be used to calculate significant financial key figures. For the IT-Business-alignment these are especially the Total Cost of Ownership (TCO) and the Return on Investment (ROI) [53]. This method was expanded, for example by vom Brocke for the Service-Oriented Process Controlling (SOPC) [55]. Before the monetary valuation in the context of the use of SOA starts, a qualitative valuation to coordinate the infrastructure, services and activities is inserted. Trough this, only such alternatives that fulfill the defined minimum requirements, are evaluated [56]. This expandability shows that in the context of IT-security not only monetary but also qualitative aspects are considered in the decision process.

2.3. Processes as foundation of decision support in IT-security management. Due to the circumstance that the impacts of IT-security investment measures, alike all IT investments, firstly can be observed on the processes [23], the latter should—in analogy to business management—represent the focal point of security management [36-39]. Process orientation in the context of security management allows an analysis of the risk potential of incidents on value adding activities allows for the determination of the potential losses. Measures and damages, etc. can be stochastically incorporated into an appropriate combination of fault tree and event tree analysis—while the fault tree analysis maps loss occurrences, their respective impacts on the processes are modeled by means of an event tree analysis [57]. This proceeding is known from different contexts, e.g. within the scope of the failure modes and effects analysis (FMEA) or the hazard analysis critical control point method [58-60]. Due to space restrictions however, the proceeding cannot be elaborated on in greater detail at this point, especially as there is further research demand with respect to the explicit design.

Besides, the process models via the respective contributions for achievement and resource strain also allow for a mapping of the financial implications of the measures. This advance analogously takes place in the field of activity-based costing, although due to the investment character, here payments and disbursements instead of costs and activities as periodical values should be in the focus. Also it has already been described in other contexts in the form of a process-oriented investment appraisal [61-63]. The decision situation of an IT-security investment is determined, in addition to direct payments and disbursements such as the alteration of the expected loss, by the need to consider all indirect payments which are caused by making the investment [22]. Besides, additional revenues should be considered also, for example resulting from an increase of prospects acquisition due to a visibly higher security level (e.g. an SSL encryption for an online shop). Similarly, different process designs cause different cash flows. This notion is facilitated by the explicated proceeding in the sense that in addition to varying packages of measures, advanced implications such as changes in productivity may be analyzed bases on different process designs. The method of Grob and vom Brocke was already adopted for IT-security Investments [64]. Based on the presented findings, a procedure model shall be introduced in the following, by means of which investment alternatives for IT-security measures can be assessed by the presented method.

3. Procedure model for IT-risk management based on process models.

3.1. Basic procedure model of IT-risk management. The IT-risk management deals with risks resulting from the usage of information systems in a company.

The procedure of tasks is oriented at the general process of risk management [65]. In contrast, a specialized IT-security management emerged which focuses on a faultless service of the companies information system. The IT-security management traditionally focuses on the consideration of technical systems. Besides conceptual fuzziness existing, the analysis of threats within the scope of IT-security management occasionally is called risk management [66] On the basis of this process the advantages resulting from an integration of IT-risk und security management are evident Firstly the strategy and the goals of IT-risk management are to be determined in the context of the risk strategy [65]. According to these goals potential risks for the enterprise need to be identified and to be evaluated by an IT-risk analysis [38]. The IT-risk analysis serves as a basis for identifying and implementing measures for the risk governance. At this point it is obvious, that this can only achieved with the competence of IT-security management. In the classical operational risk management IT-risks usually are identified in various categories, but often not quantified [67]. However, the quantification is only possible by the cooperation of central actors and decentralized security experts, since the effects of IT-risks on the business processes need to be assessed in this way [22]. The complete procedure model is illustrated in Fig. 1.

Focusing on business processes has been claimed repeatedly for the IT-security management [36-39; 68], but has not been realized in practice yet. A risk governance basically can be achieved by avoiding (refraining from activities), passing (transfer, e.g. insurance), decreasing (protective and preventive measures) or accepting (sustaining) risks [69]. In the context of information systems these measures can be conducted by IT-security experts because of their competences [70]. Even so, an overall view has to be taken to allocate resources on the ideal security level from the organization’s point of view [1]. The risk control serves as the control of result of the risk governance and is the foundation for planning future measures in terms of a risk controlling. Reports have to be created comprehensively in accordance with the reporting duties. In a largely decentralized IT-security management a standardized ascertainment is certainly rare [1]. Furthermore proactive budgeting processes should be designed which account for the defense of potential threats and ensure that no means are assigned after developed incidents.

3.2. The procedure model for IT-risk management based on process models. The present procedure model will be instantiated in the following for the appliance of process model. For this purpose the approach must be classified according the general risk management process and then checked on the basis of special requirements of IT- security. Besides, the procedure models are linked to the established concepts of risk oriented process management and risk management [71-75]. The Security goals for analysis of Information Security were usually more or less intuitional or independently defined with the aid of standardized criteria and related questions without consideration of discrete Security goals of company. If necessary for the planning of the security level or prioritization of measures it is connected to the value of relevant objects [76]. In consideration of immaterial nature and the complexity of value definition of such important for the Information system object as "Information" this procedure is difficult to resolve and can have many-valued solution [77]. The process orientation allows both focusing on the superior business objectives, which identify contributions and goals of processes [36; 38; 74; 78] and using of supporting IT and therefore to make decision about required kind and security measures. The basal security goals to define are Confidentially, Integrity and Availability, which also must be defined in consideration of their specification on the basis of requirements of business process [35].

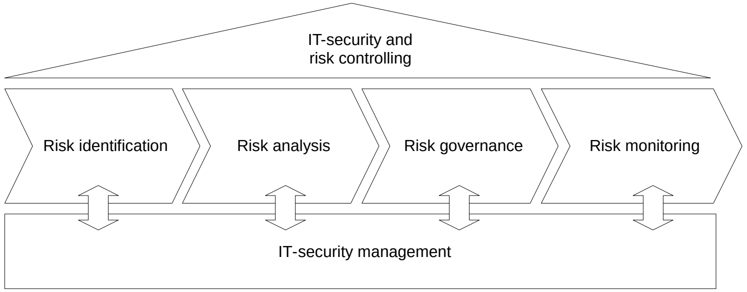

Fig. 1. The processes of IT-risk management and IT-security Management

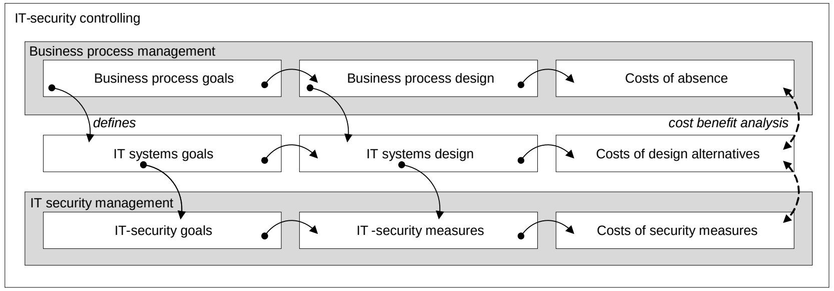

Fig. 2. Decision areas within the process of IT-risk management

Zur Mühlen und Rosemann apply for this purpose the risk-goal-model, where risks are shown opposing to process goals [74]. The costs of security measures, IT- infrastructure, income and expected losses in case of failures, which are the result of business process, are also presentable in this context. So it is obvious, that design and costs result from goal definition also as system und security goals and design have to be found according to the business processes (goals). The different aspects of the decision situation and their interdependencies are illustrated in Fig. 2. The required measures could be identified, prioritized and realized in connection with expected costs and savings according to the presented approach by Grob and vom Brocke [52]. This approach must be improved to meet the particularities by consideration of IT- security: in the foreground of all considerations is the business process, goals and direct requirements to information systems. The attention will be focused at dependency of important business processes on IT- systems. It is unacceptable to take the risk of very seldom failure, which could have however fatal effects even if the moderate expectancy value implicates this. There isn't simple exchange relationship between the higher security level and the higher security price, as it often supposed considered to be [77].

3.3. Refining the procedure model for critical infrastructures. Moreover, in most relevant IT- risk and security management frameworks there are several compromise classes to discern [79-82]. A criticality analysis or Business Impact Analysis is usually carried out within the bounds of risk identification and risk analysis, and on its basis there are critical business processes and the appropriate information systems (critical IT-infrastructure) to be identified. Therefore, it is recommended to fulfill different measures planning for business processes and associated information systems with normal risk disposition and critical business processes and underlying critical IT- infrastructures (e.g. data center). By the information system with normal risk disposition according to the BSI Baseline Protection the adaption of presented approach to profitability analysis of process models by Grob et al. is applied [64]. It must be taken into consideration, that critical infrastructure are to complex and to important, as only measures with economic aspects, but rather here the main focus is on the highest security level attainability. The procedure is shown on the Fig. 3.

The critical analysis is an approach for identification of critical business processes [83]. The analysis tries to identify the relevance of business processes, and to analyze how the single failures can affects the whole process. If there are fatal consequences appeared, this process is considered to be critical. The "Joint Standards" are the accumulation of standards, that were published for the first time in 1997 by Business Continuity Institute (BCI) and Disaster

Recovery Institute International (DRII) for Business Impact Analysis (BIA) [80; 84]. These standards must serve as the requirements catalogue for companies in order to establish Business Continuity Management in the company. The BCM's goal is to prepare the company for a crisis situation. An exemplarily application is described in the Report of Gartner Group [85]. In case of critical analysis, business processes and each information system that is to be applied for corresponding process are assigned to different categories. Seibold proposes the classification in 3 to 6 groups [83], what complies with most approaches from theory and praxis like IT- Baseline Protection and BIA [78-84; 86]. In his example he makes a classification in four classes A-D, where the processes of A class cause fatal consequences in one day, class B – in 3 days and the processes of D class have no fatal consequences at all. This classification can be described by a risk map [57].

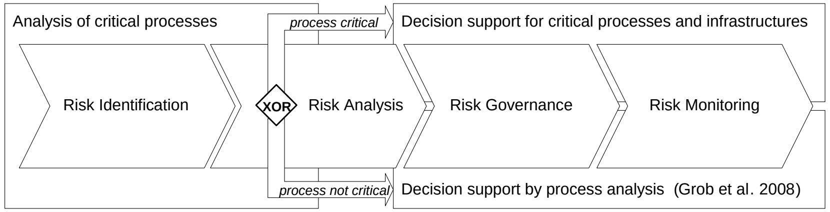
Analysis of critical processes
process critical
Decision support for critical processes and infrastructures
Risk Identification
XOR
Risk Analysis
Risk Governance
Risk Monitoring
process not critical
Decision support by process analysis (Grob et al. 2008)

Fig. 3. Procedure model for IT-risk management regarding critical infrastructures.

First of all, all business processes of the company have to be identified and described, moreover all connections to other processes must be identified. For each business process the risk potential must be identified. If business processes depend on other processes, their risks must be taken into consideration by risk evaluation until the total risk potential is identified. If the other business processes depend on analyzed process, the total risk potential of this process must be forwarded to corresponding processes to make the identification of the total risk potential possible for those processes too. The procedure model considers also the above-mentioned interdependence of business processes and information systems. But it may lead to difficult-to-resolve cycles especially if the Model has high interdependence of business processes and information systems. It can be met with established approaches of complexity management in context of process models [87].

The information systems accompanying the critical commercial processes are called here as critical infrastructures. The other choice of measures takes place here is about a criterion catalogue to be configured for the isolated case. The most important extension to above is that particular criteria can be defined as absolutely necessary (so-called lethal criteria). In the case of non-fulfillment of one of these criteria, the necessary protection of the critical infrastructure as a whole is not guaranteed. The use of the criteria catalogue follows itself a procedure model. The procedural model follows the procedure model of the IT-Baseline Protection Methodology [82]. At first a danger and requirement analysis should be carried out, in order to parameterize the criterion system. This configuration of the criterion catalogue serves to fade out superfluous elements of the catalogue. In the context of the assessment of the examined systems, a weak point analysis should be carried out. The criterion catalogue contributes to identify weak points to be repaired, in which it reproaches a huge number of measures for lethal criteria, which are not fulfilled and have thus top priority. In the connection, all possible measures, which can be carried out, are arranged for the improvement of other areas from the criterion catalogue. The choice of the measures to be carried out is determined in the phase of risk governance, by means of a modified cost-benefit-model. Trough this, only such alternatives that fulfill the defined minimum requirements, are part of the allowed portfolios of the necessary measures [56]. The portfolio, which shows the slightest TCO, is selected. Other (more expensive) portfolios can be taken into consideration in the frame of a "bargaining solution" if these don't fulfill lethal criteria in higher measure.

4. Outlook. With this paper, a procedure model for the decision support of IT-security investments has been introduced. The evaluation of the state-of-the-art in the field of IT-security management has illustrated that existent approaches are either not practice oriented and hence not relevant for the practice or – as has been demonstrated with regard to the ROSI – lack the theoretic foundation and owing to an inadequate information summarization may lead to wrong decision recommendations. To get a methodical foundation, IT-Business-alignment concepts where evaluated. For this, technical and methodological requirements were stated. Since IT-security investments primarily exhibit a direct impact on the organizational processes, the latter are in the focus of the suggested method. Starting from an integrated view on risks, security measures and benefits, payments and disbursements of all processes affected by a designated bundle of measures are determined. Existing approaches were integrated into a generic proceeding model for IT-risk management. In addition to that the necessity of a distinction between such methods for regular and critical business processes was shown. After a refinement of the procedure for critical business processes requirements for decision support in this context were developed. Future research should focus on the development of a criteria catalogue for critical infrastructure.

References: **1.** *M. Falk, M. Hofmann.* Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben. Arbeitspapiere Wirtschaftsinformatik, Arbeitspapiere WirtschaftsinformatikJustus-Liebig-Universität Gießen, Gießen, 2006. **2.** *J. A. Hall, S. L. Liedthka.* The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing // Communications of the ACM, 50 (3):95-102, 2007. **3.** *J. A. Hall.* The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing, Communications of the ACM, 2007. **4.** *L. Lensdorf, U. Steger.* IT-Compliance im Unternehmen, Der IT-Rechtsberater:206-210, 2006. **5.** *BSI.* Kosten und Nutzen der IS-Sicherheit, Studie des BSI zur Technikfolgen-Abschätzung, 2000. **6.** *P. Fettke.* State-of-the-Art des State-of-the-Art - Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik // Wirtschaftsinformatik, 48 (4):257-266, 2006. **7.** *M. Kütz.* IS Controlling für die Praxis. Konzeption und Methoden, dpunkt, Heidelberg, 2005. **8.** *N. Pohlmann.* Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? // Wirtschaftsinformatik, 43 (248):26-34, 2006. **9.** *T. R. Peltier.* Information security risk analysis, Auerbach Publications, Boca Raton, 2001. **10.** *E. Brynjolfsson.* The productivity paradox of information technology // Communications of the ACM, 36 (12):66-77, 1993. **11.** *E. Brynjolfsson, L. Hitt.* Paradox lost? Firm-level evidence on the returns to information systems spending // Management Science, 42 (4):541-588, 1996. **12.** *J. N. Luftman.* Key issues for IT executives // MIS Quarterly Executive, 3 (2):1-18, 2004. **13.** *N. Carr.* IT doesn't matter // Harvard Business Review, 81 (5):41–49, 2003. **14.** *R. Vossbein.* Datenschutz-Controlling – Den Wirtschaftsfaktor Datenschutz effizient planen, steuern und kontrollieren, Ingelheim, 2002. **15.** *G. Rodewald.* Aligning information security investments with a firm's risk tolerance, 2nd annual conference on Information security curriculum development (Ed, Whitman, M. E.) Kennesaw, GA:139-141, 2005. **16.** *J. McCumber.* Assessing and managing security risk in IT systems: a structured methodology, Auerbach Publications, Boca Raton, 2005. **17.** *K. J. Soo Hoo.* How much is enough? A risk management approach to computer security, Consortium for Research on Information Security and Policy (CRISP), Stanford, 2000. **18.** *R. Bromme, R. Jucks, R. Rambow.* Wissenskommunikation über Fächergrenzen: Ein Trainingsprogramm // Wirtschaftspsychologie, (3):94-102, 2003. **19.** *J. vom Brocke, H. L. Grob, C. Buddendick, G. Strauch.* Return on Security Investments. Towards a Methodological Foundation of Measurement Systems (im Erscheinen), 13th Americas Conference on Information Systems (AMCIS 2007) Keystone, 2007. **20.** *U. Faisst, O. Prokein, N. Wegmann.* Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen // ZfB, 77 (5):511-538, 2007. **21.** *T. Nowey, H. Federrath, C. Klein, K. Plößl.* Ansätze zur Evaluierung von Sicherheitsinvestitionen. Sicherheit 2005", Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, In Lecture Notes in Informatics (P-62):15-26, 2005. **22.** *T. Neubauer, M. Klemen, S. Biffl.* Business process-based valuation of IT-security, Seventh international workshop on Economics-driven software engineering research (Ed, Sullivan, K.) St. Louis:1- 5, 2005. **23.** *P. Tallon.* A Process-oriented Perspective on the Alignment of Information Technology and Business Strategy // Journal of Management Information Systems (JMIS), ((im Erscheinen)), 2008. **24.** *J. Henderson, N. Venkatramen.* A Model for Organisational Transformation, In Transforming Organisations(eds, Kochan, T. and Unseem, M.) Oxford University Press, New York, NY, USA:97-117, 1992. **25.** *J. N. Luftman, P. R. Lewis, S. H. Oldach.* Transforming the enterprise: The alignment of business and information technology strategies // IBM Systems Journal, 32 (1):198-221, 1993. **26.** *R. Fischer, R. Winter.* Ein hierarchischer, architekturbasierter Ansatz zur Unterstützung des IT/Business Alignment, 8. Internationale Tagung Wirtschaftsinformatik 2007 eOrganisation: Service-, Prozess-, Market-Engineering, Vol. 2 (Eds, Oberweis, A., Weinhardt, C., Gimpel, H., et al.) Universitätsverlag Karlsruhe, Karlsruhe:163-180, 2007. **27.** *J. M. Burn.* Information systems strategies and the management of organizational change - a strategic alignment model // Journal of Information Technology, 8 (4):205, 1993. **28.** *R. Maes, D. Rijsenbrij, O. Truijens, H. Goedvolk.* Redefining business - IT alignment through a unified framework, PrimaVera Working PaperUniversiteit van Amsterdam, Amsterdam, The Netherlands, 2000. **29.** *J. C. Henderson, N. Venkatraman.* Strategic Alignment: Leveraging Information Technology for Transforming Organizations // IBM Systems Journal, 32 (1):4-16, 1993. **30.** *M. E. Porter, V. E. Millar.* How Information Gives You Competitive Advantage // Harvard Business Review, 63 (4):149-160, 1985. **31.** *B. Cumps, D. Martens, M. De Backer, R. Haesen, S. Viaene, G. Dedene, B. Baesens, M. Snoeck.* Predicting business/ICT alignment with AntMiner+, FETEW Research Report Department of Descision Sciences and Information Management (KBI), K.U.Leuven, Leuven, Belgium, 2007. **32.** *M. Broadbent, P. Weill, D. St. Clair.* The Implications of Information Technology Infrastructure for Business Process Redesign // MIS Quarterly, 23 (2):159-182, 1999. **33.** *B. H. Reich, I. Benbasat.* Measuring the Linkage Between Business and Information Technology Objectives // MIS Quarterly, 20 (1):55-81, 1996. **34.** *R. Sabherwal, R. Hirschheim, T. Goles.* The Dynamics of Alignment: Insights g´from a Punctuated Equilibrium Model // Organizational Science 12 (2):179-192, 2001. **35.** *R. L. Krutz, R. Vinces, D.* . The CISSP Prep. Guide, Wiley, 2003. **36.** *S. Röhrig.* Using Process Models to Analyse IT Security Requirements, Dissertation, Zürich, 2003. **37.** *S. Sitzberger, T. Nowey.* Lernen vom Business Engineering - Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement, Multikonferenz Wirtschaftsinformatik 2006, Vol. Tagungsband 2 (Eds, Lehner, F., Nösekabel, H. and Kleinschmidt, P.) Berlin:155-165, 2006. **38.** *P. Konrad.* Geschäftsprozeßorientierte Simulation der Informationssicherheit: Entwicklung und empirische Evaluation eines Systems zur Unterstützung des Sicherheitsmanagements, Dissertation, Köln, 1998. **39.** *S. Jakoubi, S. Tjoa, G. Quirchmayr.* Rope: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes, Fifteenth European Conference on Information Systems (Eds, Österle, H., Schelp, J. and Winter, R.) St. Gallen:1596-1607, 2007. **40.** *J. vom Brocke, C. Buddendick.* Security Awareness Management, Konzeption, Methoden und Anwendung, 7. Internationale Tagung Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety (Eds, Ferstl, O. K., Sinz, E. J., Eckert, S., et al.) Bamberg:1227-1246, 2005. **41.** *P. P. Tallon.* Does IT pay to focus? An analysis of IT business value under single and multi-focused business strategies // Journal of Strategic Information Systems, 16 (3):278-300, 2007. **42.** *R. Winter, K. Landert.* IT/Business Alignment als Managementherausforderung // Wirtschaftsinformatik, 48 (5):309, 2006. **43.** *W. M. P. van der Aalst.* Business alignment: using process mining as a tool for Delta analysis and conformance testing // Requirements Engineering, 10 (3):198-211, 2005. **44.** *H. L. Grob, F. Bensberg.* Kosten- und Leistungsrechnung, Vahlen, Müchen, 2005. **45.** *H. L. Grob, S. Volck.* Abbildung von Geschäftsprozessen mit ereignisgesteuerten Prozeßketten. // Wirtschaftswissenschaftliches Studium (WiSt), 24 (11):604-608, 1995. **46.** *F. Abolhassan, T. Beck.* Performance Measurement als Voraussetzung für Business Process Excellence, In Business Engineering in der Praxis:361-377, 2005. **47.** *H. Heß.* Monitoring, Analyse und Optimierung der Unternehmens-Performance — State of the Art und aktuelle Trends, In AGILITÄT durch ARIS Geschäfprozessmanagement(eds, Scheer, A.-W., Kruppke, H., Jost, W., et al.) Springer, Berlin et al.:245-260, 2006. **48.** *B. Dinter, T. Bucher.* Business Performance Management, In Analytische Informationssysteme(eds, Chamoni, P. and Gluchowski, P.) Springer, Berlin et al.:23-50, 2006. **49.** *R. S. Kaplan, D. P. Norton.* The Balanced Scorecard-Measures that Drive Performance // Harvard Business Review, 70 (1):71-79, 1992. **50.** *M. Löcker.* Integration der Prozesskostenrechnung in ein ganzheitliches Prozess- und Kostenmanagement, Logos, Berlin, 2007. **51.** *T. Allweyer.* Geschäftsprozessmanagement. Strategie, Entwurf, Implementierung, Controlling., W3L-Verlag, Herdecke, 2005. **52.** *H. L. Grob, J. vom Brocke.* Controlling des Designs von Logistikprozessen., In Logistik Management, Springer Expertensystem Logistik Management(eds, Baumgarten, H., Becker, J., Wiendahl, H.-P., et al.) Berlin:1-26, 2004. **53.** *H. L. Grob.* Einführung in die Investitionsrechnung. Eine Fallstudiengeschichte, Vahlen, München, 2006. **54.** *H. L. Grob.* Investitionsrechnung auf der Grundlage vollständiger Finanzpläne – Vorteilhaftigkeitsanalyse für ein einzelnes Investitionsobjekt // WISU - Das Wirtschaftsstudium, 13 (1):16-23, 1984. **55.** *J. vom Brocke.* Serviceorientierte Architekturen, Management und Controlling von Geschäftsprozessen, Vahlen, München, 2007. **56.** *H. L. Grob.* Das Preis-Leistungsmodell, Arbeitsberichte des Lehrstuhls für Wirtschaftsinformatik und Controlling in der Reihe "Computergestütztes Controlling"(Ed, Grob, H. L.) Münster, 2003. **57.** *H.-P. Königs.* IT-Risiko-Management mit System. Von den Grundlagen bis zur Realisierung – Ein praxisorientierter Leitfaden, Wiesbaden, 2005. **58.** *W. D. Franke.* FMEA, Landsberg/Lech, 1989. **59.** *W. Schneeweiss.* Die Fehlerbaum-Methode. Aus dem Themenkreis Zuverlässigkeits- und Sicherheits-Technik, Hagen, 1999. **60.** *K. Pichardt.* Qualitätsmanagement Lebensmittel: vom Rohstoff bis zum Fertigprodukt, Heidelberg, 1997. **61.** *S. Küker, H.-D. Haasis.* Geschäftsprozeßmodellierung als Basis einer informationswirtschaftlichen Unterstützung für ein AQU-Management, Umweltinformatik 99 (Eds, Rautenstrauch, C. and Schenk, M.):256-268, 1999. **62.** *A. Müller, L. von Thienen, H. Schröder.* IT-Controlling: So messen Sie den Beitrag der Informationstechnologie zum Unternehmenserfolg, Arbeitspapiere der NordakademieElmshorn, 2004. **63.** *R. Kesten, H. Schröder, A. Wozniak.* Konzept zur Nutzenbewertung von IT-Investitionen, Arbeitspapiere der NordakademieElmshorn, 2006. **64.** *H. L. Grob, G. Strauch, C. Buddendick.* Conceptual Design of a Method to Support IS Security Investment Decisions, International Conference on Information Systems Technology and its Applications (ISTA 08)Kop, Christian Kaschek, Roland, Klagenfurt, 2008. **65.** *H. Krcmar.* Informationsmanagement, Heidelberg, 2003. **66.** *K. Schmidt.* Der IR Security Manager, München, 2006. **67.** *C. Locher.* Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement, Innovationen im Retail-Banking: der Weg zum erfolgreichen PrivatkundengeschäftWeinheim:477-498, 2005. **68.** *J. vom Brocke.* Referenzmodellierung, Gestaltung und Verteilung von Konstruktionsprozessen, Logos Verlag, Berlin, 2003. **69.** *T. Mai.* Management der Organisation. Organisation der Sicherheit, München, 2003. **70.** *H.-P. Nägeli.* Management der Informationssicherheit – Erfahrungen eines Finanzdiensteleisters, Strategisches IT-Management(Ed, Brenner, W. M., A.; Zarnekow, R. Hrsg) Heidelberg:79-88, 2003. **71.** *E. Brabander, H. Ochs.* Analyse und Gestaltung prozessorientierter Risikomanagementsysteme mit Ereignisgesteuerten Prozessketten., Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten (EPK 2002) (Eds, Nüttgens, M. and Rump, F.) Trier:17-35, 2002. **72.** *M. Diederichs.* Risikomanagement und Risikocontrolling, Vahlen, München, 2004. **73.** *L. Hengmith.* Geschäftsprozessmodellierung und -simulation als Hilfsmittel zum Management operationeller Risiken // Banking and Information Technology, 6 (2):17–29, 2005. **74.** *M. zur Muehlen, M. Rosemann.* Integrating Risks in Business Process Models, Australasian Conference on Information Systems (ACIS 2005) Manly, Sydney, 2005. **75.** *T. Rieke.* Prozessorientiertes Risikomanagement. Ein informationsmodellorientierter Ansatz., Wirtschaftswissenschaftliche Fakultät Westfälische Wilhelms-Universität Münster, Münster, 2008. **76.** *J. M. Carroll.* Computer Security, Boston 1996. **77.** *V. Le Veque.* Information Security - a Strategic Approach, Wiley, Hoboken, 2006. **78.** *S. Kairab.* A Practical Guide to Security Assesments, Auerbach, Boca Raton, 2005. **79.** *C. o. S. O. t. t. T. C. COSO.* Enterprise Risk Management - Integrated Framework. Executive Summary, (Ed, Commission, C. o. S. O. t. t. T.):16, 2004. **80.** *BCI.* Business Continuity Management - Good Practice, (Ed, Institute, T. B. C.), 2005. **81.** *BSI.* BSI-Standard 100-2: IT-Baseline Protection Methodology, (Ed, BSI), 2005. **82.** *BSI.* IT-Baseline Protection Catalogues, Bonn, 2007. **83.** *H. Seibold.* IT-Risikomanagement, Oldenbourg Wissenschaftsverlag, München, 2006. **84.** *R. Von Rössing.* Betriebliches Kontinuitätsmanagement, mitp Verlag, Bonn, 2005. **85.** *G. Group.* A report for Sample Company, Business Impact Analysis, 2002. **86.** *BSI.* BSI-Standards 100-3: Risk Analysis based on IT-Baseline Protection, (Ed, BSI):19, 2005. **87.** *M. Rosemann.* Komplexitätsmanagement in Prozeßmodellen. Methodenspezifische Gestaltungsempfehlungen für die Informationsmodellierung, Wiesbaden, 1996.

Поступила в редколлегию 20.02.08

UDC 681.518

M. HELFERT, PhD, MSc, BSc, Dublin City University,
Markus.Helfert@computing.dcu.ie
S. DZHUMALIEVA, MSc, BSc, Dublin City University,
Stefka.Dzhumalieva2@mail.dcu.ie

INTRODUCING PROCESS MANAGEMENT IN E-GOVERNMENT AND HEALTHCARE

Відкритий сектор економіки має, у порівнянні з іншими секторами, відносно недостатньо розвинену структуру інформаційних систем. У цьому контексті є сенс вважати важливими зниження витрат та спрямлення робочих потоків. Проте, незважаючи на важливість управління процесами, у теперішній час є дуже мало керівних документів, які допомагають впровадити управління процесами у користувальницьку адміністрацію. Мета цієї роботи – дати огляд можливої інфраструктури для аналізу проектів з управління процесами. Шляхом використання цієї інфраструктури ми аналізуємо систему управління у Болгарії та адміністрування охороною здоров‘я у Ірландії. Наш аналіз дав деякі цікаві результати.

The public sector has shown that it has, compared with other sectors, a relatively underdeveloped information system structure. In this context the importance of reducing costs and streamlining workflows and processes is ever more recognized. However, despite the importance of process management, currently there are internationally very few guidelines provided for introducing process management in public administration. The objective of this paper is to outline a framework for analyzing process management projects. By using this framework we analyze a system in the public administration of Bulgaria as well as an implementation of a healthcare administration system in Ireland. Our analysis revealed some interesting results. The reasons for failure in public administration are rather content and structural in nature then solely project management issues.

1. Introduction. In order to improve the efficiency and effectiveness of the public sector a number of reform initiatives emerged over the last two decades [6]. Influenced by the rapid advancement of information and communication technologies (ICT) the introduction of effective information systems became the primary mean for increased efficiency and effectiveness in the public sector. In order to modernize public management many organizations have implemented new ICT systems. Innovative solutions for communicating with citizens are broadly referred to as electronic government (e-government), digital government, electronic administration [2] or in the case of healthcare e-health. In this context many organizations and researchers emphasize the importance of introducing process management and redesigning processes. Among many challenges, most stress interoperability of information and communication systems and the link to processes that they support as crucial [32].

The concept of interoperability encompassed interactions at local, national and international level. It requires organizational, semantic and technical inter-