

Assessing the Effects of IT Changes on IT Risk – A Business Process-Oriented View

Stefan Sackmann

Institute of Computer Science and Social Studies, Dept. of Telematics
University of Freiburg
Friedrichstr. 50
79098 Freiburg, Germany
sackmann@iig.uni-freiburg.de

Abstract: The economic relevance of IT risk is increasing due to various operational, technical as well as regulatory reasons. Increasing flexibility of business processes and rising dependability on IT require continuous risk assessment, challenging current methods of risk management. Extending these methods by a business process-oriented view is a promising approach for taking the occurring dynamics and interlinks into consideration. In this contribution, a layer based approach for systematic modeling of relations between causes (threats) and effects (direct and indirect loss) is pursued. On the basis of these cause-effect relations, the presented IT Risk Indicator *InTRIn* measures changes in the IT support of business processes. It is discussed how *InTRIn* can provide accurate and real-time information on the IT risk situation and thus improve IT risk management.

1 Flexible Business Processes and IT Risk

The flexibility to adapt business processes to customers' changing demands is regarded as an important instrument for companies in order to be able to distinguish themselves from their competitors (e.g. [Sa95; BG05; Mi07]). To create flexibility, information technology adopts an increasingly supportive role. While, at least in Germany, two out of three companies already use IT systems such as ERP or SCM to manage their business processes [Sa05], the need for flexibility is further reinforced by current technological trends. The increasing operational use of web services and the realization of service-oriented architectures (SOA), as well as the use of virtualization approaches or so-called services on demand, provide a helpful and suitable IT infrastructure [Mi07; Kr05].

However, increasing automation of business processes by relying on a flexible IT infrastructure does not only improve business process performance but also places particular emphasis on IT risk. On the one hand, business processes are directly linked with a company's economic return as well as compliance with regulations, contracts, and standards [LK06] [Ka08]. Increasing dependency of business processes on IT also increases the possible indirect losses resulting from a malfunction of IT that can easily

exceed the direct ones. On the other hand, flexibility of business processes and context-specific adaptation make it almost impossible to predefine all possible workflows and the associated IT risk. The assessment of this risk also has to take fast changing specifications of interlinked IT into consideration. Under these circumstances, providing management with accurate risk information at any time means new challenges to current risk management methods. However, IT is not only the origin of new risk but also a promising starting point for assessing and managing it.

This paper presents an approach for measuring changes in the flexible IT infrastructure underlying a business process. Therefore, after a short discussion of the increasing relevance of IT risk resulting from flexible business processes, a layer model is presented in section 2. Its suitability for modeling relations between causes of IT risk and their effects on a company's results is discussed. In section 3, the IT Risk Indicator *InTRIn* as measure for changes in the cause-effect relation is introduced. It is discussed, how this measure can be used for assessing effects of changes in the IT infrastructure on IT risk. The contribution closes with a short conclusion and outlook identifying open research issues in the field of business process-oriented IT risk management.

2 Modeling Cause-Effect Relations for IT Risk

2.1 Flexible Business Processes and IT Infrastructure Challenge Risk Management

There is no common definition of IT risk in related literature. While some authors (e.g. [BSI05]; [MR05]) define IT risk as the probability of damage excluding the amount of loss, other authors (e.g. [Pa07]) concentrate on the so-called "long tail" risks that occur with low frequency and high impact. From a value-oriented view, IT risk is seen as a part of operational risks measuring the unexpected losses that are determined by the frequency and amount of losses, e.g., by their value at risk [JR01] [Ho03]. Such a loss-oriented view is suitable for IT risk and thus taken up in this contribution.

The trends of current developments unquestionably lead to an increasing economic significance of IT risk: IT is becoming increasingly important for an efficient production of goods and services as well as for the efficient coordination of business activities in a increasing interlinked economy. In both fields, a disturbance of IT can cause persistent business failure within a short time. Furthermore, an increasing regulation (e.g. Sarbanes-Oxley Act, Basel II), (quasi-)standards (e.g. Cobit, ITIL), and contractual agreements (e.g. outsourcing, service level agreement) raise the significance of IT risk for companies and make explicit demands on IT risk management. Last but not least, an increasing number of known vulnerabilities [Go06] as well as developing attacks (e.g. phishing, pharming) and limited capabilities of security mechanisms are continuously threatening interlinked information systems [Wh03]). Bringing all these trends together, the management of IT risk resulting from the operational use of IT is more than a current hype. The increasing relevance of IT risk also means an increasing need for risk management.

At best, a quantification of IT risk reverts to a set of past cases of loss collected over several periods [McN05]. As long as the relation between causes and effects remains relatively constant, the expected frequency and amount of losses can be derived by interpolation from an analysis of the individual cases collected. However, each change of the relations between causes and effects makes such past data increasingly inaccurate. Strictly spoken, each slight change requires a revaluation of the “historical” data basis according to the changes and, consequently, a new quantification of the risks under consideration. Currently, such modifications are usually made indirectly by a manual, “expert”-based overall adjustment of either the distributions of frequency of loss cases or the distribution of loss amounts. In the context of flexible business processes and a flexible adaptation of the underlying IT infrastructure, such overall adjustment mechanisms are challenged by at least the following three points:

- (1) Fast developing IT makes it difficult to rely on qualified experiences in estimating the implications of changes in IT risk and thus adequate treatment thereof in risk quantification.
- (2) The relationship between the causes of IT risk and their effects is – at least in modern companies – complex and heavily interdependent. Every threat can endanger several business processes since many IT applications are usually not used exclusively for one business process. Conversely, every business process can be endangered by several threats since business processes are usually supported by several IT applications.
- (3) The increasing flexible use of IT constantly changes the tangled relations between the causes of IT risk and their possible effects on business processes. The motives are manifold, for instance the automated patching of software bugs and vulnerabilities, the adaptation of workflows in real time to business needs, the execution of identical IT applications on different platforms in order to optimize capacity utilization (virtualization), or the flexible (re-)combination of services e.g. in SOA.

Non-consideration of these specific characteristics of flexible business processes and fast changing IT support will most likely lead to a misjudgment of a company’s “real” IT risk. Neither under- nor overestimation is optimal from a value-oriented stakeholders’ perspective. Flexible business processes require process-oriented IT risk management being capable to take also the partly, only marginally changing relations between causes and effects on the company’s results into consideration. This makes the integration of a technical as well as an economic view necessary, since events like moving an IT application from one server to another one can increase (or decrease) the probability of damage enormously without changing the functionality of the IT application from a business process view. Conversely, the integration of an existing IT application into a critical business process can enormously increase possible loss in the case of damage without changing the IT from a technical point of view.

2.2 Modeling Cause-Effect Relations with the IT Risk Reference Model

The management of IT risk requires a method for taking continuously changing cause-effect relations into consideration. For this purpose, the IT Risk Reference Model has been developed. It is structured following a hierarchical abstraction layer model as used

in computer science [Ta79] in order to reduce complexity. Each single layer encapsulates similar functionalities on a general level while hiding the implementation details. The connection between the layers is given by so-called “services” that are offered from a lower to a higher layer, keeping all subordinated layers transparent.

A layer model for IT risk requires a linking of the causes, i.e. the threats from a mainly technological point of view and the effects, i.e. the parts of a business process that are disturbed. As a first and simple approach, the proposed IT Risk Reference Model distinguishes four layers:

(I) *Business Process Layer* (BP layer): In the context of IT risk, an analyzed business process should be quantifiable according to its contribution to a company’s return that is under risk. Beginning with the economic view on IT risk, the BP layer represents the “effects”, i.e. the set of all activities of a business process that can be affected by a malfunction of IT. Business processes with their associated procedures and activities can be modeled independently from the underlying information system [Gi01], for instance with ARIS modeling tools [Sc00]. On the BP layer, enclosed activities using at least one IT application for their realization are regarded as independent elements and modeled as:

$$(1) \quad BP = \{BP_1, \dots, BP_c\} \quad \text{with } c = \text{number of elements in BP layer.}$$

(II) *IT Application Layer* (AP layer): The AP layer includes all IT applications with their underlying IT infrastructure that are used from the defined elements of the BP layer. In practice, identifying individual IT applications is a non-trivial issue and dependent on an individual company’s context. However, following a SOA approach makes the identification relatively easy because web services are inherently defined as independent applications [Cu03]. In the case of SOA, their relation to the superordinated activities of the BP layer can be automatically carried out to a very large extent by analyzing the formal “orchestration” information, e.g. in the BPEL¹ description of a company’s business processes. On the AP layer, IT applications are modeled as:

$$(2) \quad AP = \{AP_1, \dots, AP_d\} \quad \text{with } d = \text{number of elements in AP layer.}$$

At the same time, IT applications are relevant points of failure. The assignment of protection goals [MR99] to IT applications allows the bringing together of the economic with the more technological, IT security-based handling of IT risk on the basis of vulnerabilities. Consequently, vulnerabilities are the core of the next layer.

(IIIa) *Vulnerability Layer* (VN layer): The VN layer includes all vulnerabilities that are known in the IT applications of the AP layer. Vulnerabilities are seen as a “bridge” between business processes and IT threats because they are both the

¹ The *Business Process Execution Language* (BPEL) is an XML-based language for defining business processes and their implementation with web services. For more detailed information see, e.g., <http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html>.

loophole for attacks and the cause of disturbance of business processes. Vulnerabilities can be systematically identified by several methods [Ve81]. In general, top-down directed analytical search methods produce most extensive results capable of describing all known attack trails for the disturbed element in mind [Sc99]. Since vulnerabilities cannot only be found in applications but also in middleware, operating systems or hardware, they are possibly relevant for more than one IT application identified on the AP layer. Thus, vulnerabilities are interpreted as independent “elements” that can be associated to at least one IT application and formalized as:

$$(3) \quad VN = \{VN_1, \dots, VN_e\} \quad \text{with } e = \text{number of elements in VN layer.}$$

- (IIIb) *Security Mechanism Layer* (SM layer): Security mechanisms are capable of patching vulnerabilities or opposing threats. Security mechanisms are an essential part of security management, thus, the measures induced there can be used as a basis for the identification of elements on the SM layer. Since security mechanisms are not always capable of patching vulnerabilities completely, it is important to take their effectiveness into consideration when modeling the relations between causes and effects of IT risk, e.g. in the form of the general probability that an attack can be averted (e.g. [GL02]) or in the form of security levels (e.g. [FP05]). In the SM layer, the elements are security mechanisms that are able to patch vulnerabilities of the VN layer and to successfully avert attacks:

$$(4) \quad SM = \{SM_1, \dots, SM_f\} \quad \text{with } f = \text{number of elements in SM layer.}$$

- (IV) *Threat Layer* (TH layer): The TH layer includes all known threats that are seen as causes of IT risk. Threats always exist regardless of whether they are realized as attacks or not. A starting point for defining and categorizing relevant threats can be found in best-practice frameworks such as [HL98] or the IT Baseline Protection Manual [BSI05]. In the TH layer, the elements are such threats that are able to exploit vulnerabilities and formalized as:

$$(5) \quad TH = \{TH_1, \dots, TH_g\} \quad \text{with } g = \text{number of elements in TH layer.}$$

Within these layers and their elements, the basic relations between the causes and effects can be modeled providing a “snapshot” of the cause-effect relations for any time. The extension of the layers with new elements can be carried out without any problems, e.g. in the case where new activities in the business project are introduced, new IT applications are implemented or new vulnerabilities are detected, or new threats become known.

The relations between the different layers of the IT Risk Reference Model can then be formally described in the form of matrices: the relations between the business processes and the IT applications with the matrix $BPAP$, between the IT applications and the vulnerabilities with the matrix $APVN$, and between the vulnerabilities and the threats with the matrix $VNTH$.

$$(6) \quad BPAP = \begin{bmatrix} l_{1,1} & \dots & l_{c,1} \\ \dots & \dots & \dots \\ l_{1,d} & \dots & l_{e,d} \end{bmatrix} \quad APVN = \begin{bmatrix} m_{1,1} & \dots & m_{d,1} \\ \dots & \dots & \dots \\ m_{1,e} & \dots & m_{d,e} \end{bmatrix} \quad VNTH = \begin{bmatrix} n_{1,1} & \dots & n_{e,1} \\ \dots & \dots & \dots \\ n_{1,g} & \dots & n_{e,g} \end{bmatrix}$$

The SM layer is omitted in this matrix representation. Of course, it has to be taken into consideration when modeling the relation between causes and effects of IT risk. Since security mechanisms are usually associated with vulnerabilities and, in a narrower sense, they are not an independent layer making the threats transparent for vulnerabilities, they have to be considered in the relations n_{ij} between the vulnerabilities and their corresponding threats.

Applying the IT Risk Reference Model to a company's business processes and IT support requires an additional concept to define how the relations l_{ij} , m_{ij} , and n_{ij} between the elements are formally modeled. Certainly the simplest approach to define, e.g., the relation l_{ij} between the business process activity BP_i and the IT application AP_j is to model them in a binary manner as:

$$(7) \quad l_{ij} \in \{0,1\} \quad \forall i \in \{1, \dots, c\} \wedge j \in \{1, \dots, d\}$$

where "0" means "there is no relation, the business process activity BP_i does not rely on the IT application AP_j " and "1" means "there is a relation, the business process activity BP_i does rely on the IT application AP_j ".

The IT Risk Reference Model provides a systematic method for identifying and modeling the cause-effect relations in order to improve IT risk management. If required, the relations can also be described in a more precise manner, for example in the form of probabilities, probability distributions or even conditional probabilities setting up a Bayesian network. Also, expanding the IT Risk Reference Model with more detailed layers may facilitate a better and more precise view of the depicted relations between causes and effects and thus improve the estimation of IT risk. In the end, the operational trade-off between precision and the effort to get the necessary data will have to provide reasons for the type of formal description of the relations that should be ideally implemented. For a first evaluation and with automated detection and measuring of changes in mind, the binary approach is proposed for all three matrices. On a general level, this does not change the aspired modeling and systematic integration of cause-effect relations into IT risk management.

3 Measuring Changes of the Cause-Effect Relations

The IT Risk Reference Model serves as starting point for measuring changes in the cause-effect relations between threats and business processes. In a first step, every change has to be identified and measured for transforming it into accurate risk information in a second step. For measuring changes within and between the layers and modeling them in the respective matrices, their identification is a necessary precondition. The effort needed can be reduced by partial automation especially on the layers where

changes occur with high frequency, i.e. business processes and IT applications. Especially in the context of SOA, this is achievable by automated monitoring and analyzing changes of the BPEL scripts describing the “orchestration” of web services according to the requirements of business processes. For measuring the changes, the IT Risk Indicator (*InTRIn*) is presented followed by a discussion of its transformation into accurate risk information.

The risk indicator *InTRIn* is designed to measure the direct “paths” existing between the threats and the business process. Focusing on paths and not on the individual layers seems to be advantageous since, e.g., patching a vulnerability of an IT application means a change to the cause-effect relations only if the vulnerability can also be exploited by an attack. In the case where the relevant vulnerability is already protected by a security mechanism, the additional patching of the IT application has no further effect on IT risk. Thus, only these changes of the elements and relations that are also changing the paths between threat (cause) and business process (effect) are measured. Formally, the sought paths can be calculated as matrix *BPTH* by simply multiplying the matrices of the IT Risk Reference Model and normalizing it:

$$(8) \quad BPTH = \left[(c \cdot g)^{-1} \cdot (BPAP \cdot APVN \cdot VNTH) \right] = \begin{bmatrix} \lambda_{1,1} & \dots & \lambda_{c,1} \\ \dots & \dots & \dots \\ \lambda_{1,f} & \dots & \lambda_{c,g} \end{bmatrix} \quad \forall \lambda_{r,j} \in \{0,1\}$$

Furthermore, the absolute number of paths r_0 – which is later required for calculating the risk indicator *InTRIn* – can be calculated as sum of the individual elements of the matrix as follows:

$$(9) \quad r_0 = \sum_{i=1}^c \sum_{j=1}^g \lambda_{r,j}$$

It is assumed that the relevant business process and IT system are not completely infallible and at least one path exists. Thus, it is considered that $r_0 > 0$. For measuring the changes in the cause-effect relations, the matrix *BPTH* is to be calculated in its original situation $BPTH^{t=0}$ and in its situation after the change(s) occurred $BPTH^{t=1}$. The difference of the matrices then represents the changes:

$$(10) \quad \Delta BPTH = BPTH^{t=1} - BPTH^{t=0} = \begin{bmatrix} \delta_{1,1} & \dots & \delta_{c,1} \\ \dots & \dots & \dots \\ \delta_{1,f} & \dots & \delta_{c,g} \end{bmatrix} \quad \forall \delta_{i,j} \in \{-1,0,1\}$$

The targeted risk indicator *InTRIn* is calculated on the basis of this “matrix of changes” $\Delta BPTH$. A single change in the cause-effect relations can either add new paths or omit old paths whereas several changes can do both. Since an omitted path does not inevitably compensate an added one, it is appropriate to take each category of changes separately into consideration by calculating r_+ as absolute number of added paths and vice versa r_- as absolute number of omitted paths.

$$(11a) \quad r_+ = \# \{ \forall \delta_{i,j} \mid \delta_{i,j} = 1 \}$$

$$(11b) \quad r_- = \# \{ \forall \delta_{i,j} \mid \delta_{i,j} = (-1) \}$$

The risk indicator *InTRIn* is defined as the relative difference between the two matrices compared and thus calculated as follows:

$$(12a) \quad InTRIn_+ = \frac{r_0 + r_+}{r_0} \quad \text{with} \quad InTRIn_+ \geq 1$$

$$(12b) \quad InTRIn_- = \frac{r_0 - r_-}{r_0} \quad \text{with} \quad 1 \geq InTRIn_- \geq 0$$

The risk indicator *InTRIn* measures the effect of changes in the cause-effect relations on the direct relation between IT threats and the business processes. Thus, it is a simple measure for the relative changes between two different scenarios of cause-effect relations.

The targeted accurate risk information about a current business process and its underlying IT support requires, in a second step, the transformation of the risk indicator *InTRIn* into a risk measure. Assuming the quantity of external factors, e.g. the probability of an attack or the monetary loss of each minute downtime of the business process as constant, an arbitrary IT risk R^x in $t = 1$ is a function of at least its value in $t = 0$ and the changes in the cause-effect relations measured with *InTRIn*.

$$(13) \quad R_{t=1}^x = f(R_{t=0}^x, InTRIn, \dots)$$

Of course, the concrete functional relation depends on both the characteristics of the IT risk taken into consideration and the concrete situation of a company. In practice, determining the functional relation might be a challenging issue demanding experiences and learning over time. Nevertheless, since the risk indicator – as indicators in general – does not aim at precise quantification of risk, it is expected to provide a helpful “hint” and real-time information about the current IT risk situation that is not yet available. Assuming, for simplicity, a functional relation of the class

$$(14) \quad R_{t=1}^x = R_{t=0}^x \cdot \alpha \cdot InTRIn^\beta$$

then allows to calculate the minimal and maximal risk as follows:

$$(15a) \quad R_{t=1}^{x,max} = R_{t=0}^x \cdot \alpha \cdot InTRIn_+^\beta \quad \text{with} \quad \alpha > 0 \wedge \beta > 0$$

$$(15b) \quad R_{t=1}^{x,min} = R_{t=0}^x \cdot \alpha^{-1} \cdot InTRIn_-^\beta \quad \text{with} \quad \alpha > 0 \wedge \beta > 0$$

For improving the management decision basis, these results can be relatively easily integrated into existing instruments for risk management, e.g. in the well known two dimensional risk matrix, where individual risks are displayed according to their expected probability of event and their expected loss (see Figure 1).

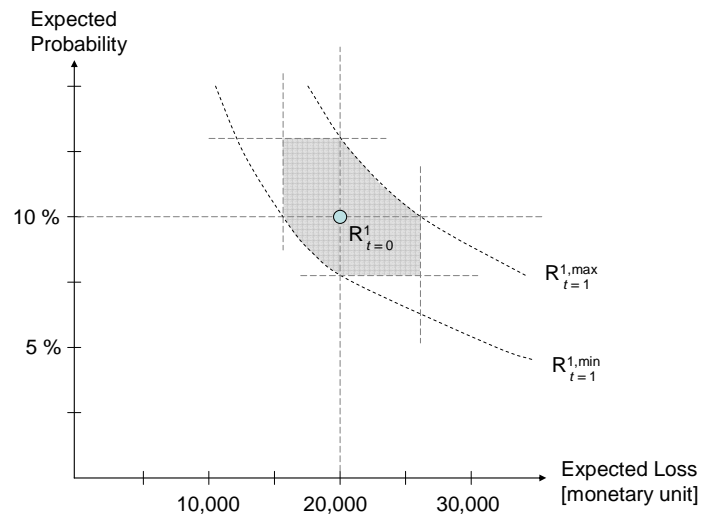


Figure 1: Visualization of the risk indicator $InTRIn$

Example: It is assumed that a company has identified and quantified the IT risk R^l (e.g. viruses) in $t=0$ with an expected loss of 20,000 monetary units and a probability of 10 %. It is further assumed that the company has identified the cause-effect relations according to the IT Risk Reference Model and calculated in $t=0$ according to equation (9) a value $r_0 = 20$. Based on this situation, one IT application that is already an element of the AP layer is newly integrated into an activity of the business process leading to six new paths and thus according to equation (12a) to $InTRIn_+ = 1.3$. At the same time, in the context of a virtualization measure for load balancing, another IT application is moved to an operating system with less vulnerabilities than the original one leading to a “cut” of four paths and thus according to equation (12b) to $InTRIn_- = 0.8$. For simplification, a functional relation of the class in equation (14) is assumed with $\alpha = 1$ und $\beta = 1$. With this information, the resultant effect on the IT risk $R_{t=0}^l$ can be estimated. According to equation (15a) and (15b), the expected maximal risk $R_{t=1}^{1,max}$ reaches a value of 2,600 units and the minimal risk $R_{t=1}^{1,min}$ a value of 1,600 units. Since the risk indicator does not differentiate between the expected probability and the expected loss, the visualization of the “new” risk $R_{t=1}^l$ in the two dimensional risk matrix corresponds to the shaded area of Figure 1. The borderline is theoretically given by the two curves of $R_{t=1}^{1,max}$ and $R_{t=1}^{1,min}$ that are the isoquantes representing all values with the same expected value of the risk. Since the interaction of the added and omitted paths is ambiguous, the two rectangles arising from the points of intersection with the lines representing the risk value at $t=0$.

Compared with current methods to estimate IT risk, i.e. knowing $R_{t=0}^l$, such a visualization of the implications of (even marginal) changes in the cause-effect relations

on IT risk provides management with additional information about current IT risk situations. Depending on the particular risk preference and the company's thresholds for acceptable risk, the result of *InTRIn* can be interpreted resulting in adequate activities. As long as $R_{l=1}^{1,max}$ is lower than the maximal acceptable risk, no action is required. If the risk area is partly above the maximal acceptable risk, the manager can decide on the basis of this information whether to provoke a laborious adaptation of risk quantification to the new situation and, if necessary, to take suitable measures.

Some limitations of the risk indicator have to be taken into consideration when using it as decision basis. Firstly, although the risk indicator *InTRIn* can measure changes in the cause-effect relations, it is an indicator in the context of IT risk. Therefore, the implications of the changes to the IT risk can only be estimated. Secondly, the different paths are all seen as being of equal importance. If there are paths more crucial for IT risk than others, this is not taken into account by the indicator. This could be remedied, e.g. by weighting the different paths, though this approach means more complexity and is part of the trade-off accuracy vs. effort. Thirdly, the assumption of binary relations between the elements of the different layers of the IT Risk Reference Model might be too restrictive. It is expected to achieve more realistic estimations of the IT risk situation when more extensive approaches as, e.g., the security level [FP05] on the layer of security mechanisms could be taken into consideration. However, this would require considering and adapting the risk indicator approach as proposed in this contribution and is subject to further research.

4 Conclusion and Outlook

The advancing realization of business processes with the support of IT means both improvements in efficiency and increased IT risk. Current economical as well as technological developments push ahead the flexibility of business processes and dynamics of the IT infrastructure. The resulting continuously changing relations between causes and effects also continuously change the IT risk. Providing management at any time with accurate information about the IT risk of a business process requires automation and extending "traditional" risk management approaches by taking the cause-effect relations into consideration.

Modeling the relations between causes and effects of IT risk in a systematic and formal way is a necessary precondition for the provision of "real-time" information about IT risk. The IT Risk Reference Model proposed in this contribution reduces the complexity of the modeling challenge by defining four layers between the causes and effects of IT risk. It connects the economic view on IT risk with the technological one and allows a formal description of the interdependencies between the separated layers in the form of expandable matrices according to a company's requirements. The IT Risk Reference Model provides a systematic basis for realizing the potential of business process-oriented IT risk management and providing management with adequate risk information at any time.

A first step to such process-oriented IT risk management is the measuring of the changes within the modeled cause-effect relations on the basis of the IT Risk Indicator *InTRIn*. This risk indicator measures the changes on the basis of paths from threats to business processes. Applying the IT Risk Reference Model and visualizing the IT risk on the basis of the risk indicator is considered feasible, since existing methods and technologies provide suitable starting points for automating the identification of changes. Extending existing instruments for risk management with this measure of changes is seen as a promising way for providing more adequate information about the current risk situation.

While the IT Risk Indicator can be realized in the short term, the integration of the cause-effect relations into all phases (identification, quantification, controlling, and monitoring) of existing risk management processes requires time for building up an adequate data basis as well as several extensions and further research: Firstly, a method for a permanent (and automated) identification of cases of loss within the business processes and the supporting IT infrastructure. Secondly, a permanent quantification of IT risk triggered by any change of the cause-effect relations. Although these extensions are still the subject of research, they can be expected to acquire a more realistic assessment of the actual IT risk situation and thus to improve risk management.

References

- [BG05] Bhatt, G. D.; Grover, V.: Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study. In: Journal of Management Information Systems, Vol. 22 (2), 2005, pp. 253-277.
- [BSI05] BSI - Federal Office for Information Security (2005): IT-Grundschutz Manual. Available at URL: <http://www.bsi.de/english/gshb/manual/download/pdfversion.zip> (2007-11-30).
- [Cu03] Curbera, F.; Khalaf, R.; Mukhi, N.; Tai, S.; Weerawarana, S.: The Next Step in Web Services. In: Communications of the ACM, Vol. 46 (10), 2003, pp. 29-35.
- [El99] Ellis, C. A.: Workflow Technology. In Beaudouin-Lafon, M.: Computer Supported Co-operative Work, John Wiley & Sons, Chichester, UK, 1999, pp. 29-54.
- [FP05] Faisst, U.; Prokein, O.: An Optimization Model for the Management of Security Risks in Banking Companies. In: Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05), 2005, pp. 266-273.
- [Gi01] Giaglis, G.M.: A taxonomy of business process modelling and information systems modelling techniques. International Journal of Flexible Manufacturing Systems, Vol. 13 (2), 2001, pp. 209-228.
- [GL02] Gordon, L. A.; Loeb, M. P.: The Economics of Information Security Investment. In: ACM Transactions on Information and System Security, Vol. 5 (4), 2002, pp. 438-457.
- [Go06] Gordon, L. A.; Loeb, M. P.; Lucyshyn, W.; Richardson, R.: CSI/FBI Computer Crime and Security Survey 2006. Computer Security Institute, 2006.
- [Ho03] Holton, G. A.: Value-at-Risk: Theory and Practice, Academic Press, San Diego, 2003.
- [HL98] Howard, J.; Longstaff, T.: A Common Language for Computer Security Incidents. Sandia National Laboratories Report SAND98-8667, 1998.
- [JR01] Jaisingh, J.; Rees, J.: Value at risk: A methodology for information security risk assessment. In: Proceedings of the INFORMS Conference on Information Systems and Technology 2001, Miami, 2001.

- [Ka08] Karagiannis, D. (2008): A Business Process-Based Modelling Extension for Regulatory Compliance. In: Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI 2008), Munich, 2008.
- [Kr06] Krafzig, D.; Banke, K.; Slama, D.: Enterprise SOA. Prentice Hall, Upper Saddle River, 2005.
- [LK06] Liebenau, J.; Kärrberg, P.: International Perspectives on Information Security Practices. London School of Economics and Political Science, McAfee, 2006.
- [McN05] McNeil, A.; Frey, R.; Embrechts, P.: Quantitative Risk Management: Concepts Techniques and Tools. Princeton University Press, Princeton, 2005.
- [Mi07] Mills, S.: The future of business – Aligning business and IT to create an enduring impact on industry. IBM, Thought leadership paper, 2007, available at URL: ftp://ftp.software.ibm.com/software/soa/pdf/future_of_business.pdf (2007-11-30).
- [MR05] Muehlen, M. zur; Rosemann, M.: Integrating Risks in Business Process Models. In: Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005), Sydney, 2005.
- [MR99] Müller, G.; Rannenberg, K.: Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy. Addison-Wesley-Longman, New York, 1999.
- [Pa07] Parker, D. B.: Risks of risk-based security. In: Communications of the ACM Vol. 50 (3), 2007, p. 120.
- [Sa05] Sackmann, S.; Strüker, J.: Electronic Commerce Enquête 2005. Konradin IT-Verlag, Leinfelden, 2005.
- [Sa95] Sanchez, R.: Strategic Flexibility in Product Competition. In: Strategic Management Journal, Vol. 16, Special Issue: Technological Transformation and the New Competitive Landscape, 1995, pp. 135-159.
- [Sc00] Scheer, A. W.: ARIS - business process modeling. 3rd ed. Berlin: Springer, 2000.
- [Sc99] Schneier, B.: Attack Trees. Dr. Dobb's Journal Vol. 24 (12), 1999, pp. 21-29.
- [Ta79] Tanenbaum, A.S.: Structured Computer Organization. Englewood Cliffs, New Jersey: Prentice-Hall, 1979.
- [Ve81] Vesely, W. E.; Goldberg, F. F.; Roberts, N. H.; Haasl, D. F.: Fault Tree Handbook. U.S. Nuclear Regulatory Commission. NUREG-0492, Washington, D.C., 1981.
- [Wh03] Whitman, M.: Enemy at the gate: Threats to information security. In: Communications of the ACM, Vol. 46 (8), 2003, pp. 91-95.