Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Adapted Loss Database – A New Approach to Assess IT Risk in Automated Business Processes

Stefan Sackmann
Martin-Luther-University Halle-Wittenberg, stefan.sackmann@wiwi.uni-halle.de

Arnt Syring
University Freiburg, arnt.syring@iig.uni-freiburg.de

Adapted Loss Database – A New Approach to Assess IT Risk in Automated Business Processes

Stefan Sackmann
Martin-Luther-University Halle-Wittenberg,
Institute for Business Informatics and Information Management
stefan.sackmann@wiwi.uni-halle.de

Arnt Syring
University Freiburg, Institute of Computer Science and Social Studies, Dpt. of Telematics
arnt.syring@iig.uni-freiburg.de

ABSTRACT

Service-oriented architectures (SOA) provide companies with dynamic IT infrastructures to adapt business processes flexibly to new requirements. However, the success of SOA will also depend on the ability to manage risk resulting from frequent and context-specific changes of IT support for automated business processes. Assessing this IT risk is challenging, since frequently changing relations between the causes of risk and their effects on business processes turns established methods for assessing risk into a game of hazard. Following a design science approach, this contribution proposes a novel approach for taking changes of cause-effect relations into consideration. Based on a backward-directed recalculation of historical loss data, a risk-adjusted loss database is generated that can provide a more realistic basis for assessing IT risk.

Keywords

IT risk, service-oriented architecture, automated business processes

CONSIDERING IT RISK – THE CHALLENGE

The ability to adapt business processes flexibly to customers' changing demands is regarded as an important attribute for companies in order to distinguish themselves from competitors and to realize competitive advantages (e.g. Brynjolfsson and Hitt, 1998; Jaisingh and Rees, 2001; McAfee and Brynjolfsson, 2008; Sanchez, 1995). Current technological developments such as service-oriented architectures (SOA), Cloud Computing, or Software as a Service provide a suitable technological basis for the automation of business processes and for gaining the aspired flexibility (e.g. Hayes, 2008; Krafzig, Banke, Slama, 2005; Mills, 2007). However, increasing automation and flexibility of business processes does not just improve business process performance. It also places particular emphasis on changing IT risk resulting from deficient and inadequate technical support of the business processes.

Present approaches for assessing risk lack methods for taking context-specific orchestration and rearrangement of services into consideration and thus inherently ignore the frequently changing relations between the causes of IT risk and its (monetary) effects on each instance of business processes. The approach presented in this contribution aims at providing management with more accurate risk information by taking flexible and frequently changing IT support explicitly into consideration.

The contribution is structured as follows: in the second section, a short definition of IT risk is given and existing approaches for assessing IT risk in a flexible IT support are discussed. Furthermore, the IT Risk Reference Model is introduced, providing a structured way to describe cause-effect relations and changes within it. Based on this model, in the third section, our proposal for organizing a loss data base and taking changes within cause-effect relations into consideration is presented. The paper closes with a short discussion on the limitations of our approach and the identification of open research issues.

MODELING CAUSE-EFFECT RELATIONS FOR IT RISKS

IT risk management focuses on the examination and assessment of risks (quantifiable and known states) rather than on uncertainties. There is no common definition of IT risk in related literature (e.g. Salvati and Diergardt, 2007). While some authors (e.g. Parker, 2007) concentrate on the so-called "long-tail" risks that occur with low frequency and high impact, the majority (e.g. BSI, 2005; Muehlen and Rosemann, 2005) define IT risk as the probability of damage excluding the amount of loss (Alter and Sherer, 2004). From a value-oriented view, IT risk is seen as a part of operational risks (Faisst and Prokein, 2008), measuring the unexpected losses that are determined by the frequency and amount of losses, e.g. by their value at risk (e.g. Holton, 2003; Jaisingh and Rees, 2001). Such a loss-oriented view is seen as suitable for IT risk and thus adopted in this contribution. In the context of automated business processes IT risks are seen as the unexpected losses resulting from deficient and inadequate technical support of the business processes, e.g. by non-availability or non-integrity of an IT service. Such IT risk can result in high financial damage, considerably outperforming other operational risks (Hechenblaikner, 2006).

Several methods are available for measuring IT risk. At best, a quantification of IT risk reverts to a set of past cases of loss collected over several periods (e.g., McNeil, A., Frey, R. and Embrechts, 2005). 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 or external data collections. However, each change makes such past data increasingly inaccurate and, strictly speaking, requires a new quantification of the risks under consideration. The usual assumption that programmed business processes are executed without error or at least with a known risk (see, e.g., (Ellis, 1999; Giaglis, 2001)) becomes increasingly unsustainable. In practice, effects of significant changes within the cause-effect relations are usually estimated by a personal, "expert"-based overall adjustment of either the distributions of frequency of loss cases or the distribution of loss amounts (see, e.g., (Gordon and Loeb, 2002; Mercuri, 2003)). Since company-specific relations between causes and effects of risks are usually neither constant nor to be described or modeled as direct correlations these approaches are insufficient for adequately assessing the actual risk situation in the context of automated and flexible business processes. For estimating "frequent and small" changes, no practical method is available yet (Sackmann, 2008a) and an adequate risk assessment mainly lacks adequate risk models and a stressable data base (Alter and Sherer, 2004; Blakely, McDermott and Geer, 2001; Jaisingh and Rees, 2001; Salvati and Diergardt, 2007). In this paper, a novel approach for modeling cause-effect-relations of IT risk and designing an according loss data base is proposed. Since this requires new methods and artifacts, our research follows the design science paradigm (Denning, 1997; Hevner, March, Park, Ram, 2004; Tsichritzis, 1998) aiming at an efficient and effective enlargement of human and organizational capabilities.

Our approach takes the current IT situation as starting point. The management of IT risk in the context of flexible business processes supported by IT requires a method for taking changing cause-effect relations directly into consideration. For this purpose, the IT Risk Reference Model has been proposed (see Figure 1) combining core aspects of IT security with process-oriented risk assessment for modeling the relations between causes, i.e. potential attacks (threats) and the effects, i.e. the parts of a business process that are disturbed. From a mainly technological and IT security view, threats could be classical security threats, such as hacker attacks or viruses. If realized, these threats result in a violation of protection goals of the supported business process, i.e. confidentiality, integrity or availability (Rörig, 2007). From a more organizational view, threats could also be malfunction of the IT, force majeure, or unsuccessful software updates (e.g. BSI, 2005).

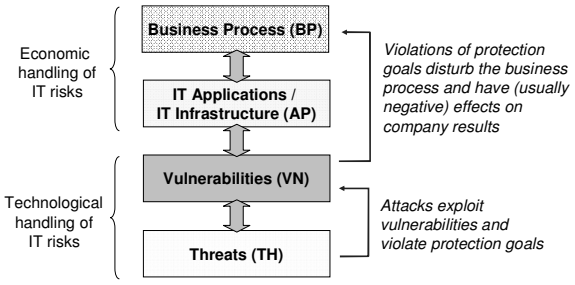

Figure 1: IT Risk Reference Model (Sackmann, 2008b)

For modeling the relations between causes and effects, our first approach distinguishes four different aspects:

1) The set of all (parts of) business processes (BP) that can be modeled with their associated procedures and activities independently from the underlying information system (Giaglis, 2001). Enclosed activities using at least one IT application for their realization are regarded as independent elements and modeled as:

(1) $BP = \{BP_1, \ldots, BP_C\}$ with C = total number of BP elements

2) The set of IT applications (AP) with their underlying IT infrastructure that are used from the defined elements of the business process. For reasons of simplicity, an aggregated view is used in this contribution. The application elements are modeled as:
   (2) $AP = \{AP1, \ldots, AP_D\}$ with D = total number of AP elements

3) Since the IT applications are relevant points of failure in the context of IT risk, vulnerabilities (VN) of the IT applications are the next group of elements. Vulnerabilities are seen as a "bridge" between business processes and IT threats because they are both the loophole for attacks and the cause of disturbance of business processes. Thus, vulnerabilities are interpreted as independent "elements" that can be associated to at least one IT application and are formalized as:
   (3) $VN = \{VN_1, \ldots, VN_E\}$ with E = total number of VN elements

4) The fourth group of elements represents all potential attacks that threaten the business processes. These threats (TH) are seen as causes of IT risk and highly related to the identified vulnerabilities. They are formalized as:
   (4) $TH = \{TH_1, \ldots, TH_F\}$ with F = total number of TH elements

Within these groups of elements, the basic relations between the causes and effects can be modeled providing a "snapshot" of the cause-effect relations for any time. It might be argued that focusing on only these four aspects on such an aggregated level is oversimplifying and, of course, business processes are more than a container for tasks as well as applications and their vulnerabilities can result from various sources like middleware, operating systems, or hardware. However, when contemplating from a data perspective, the IT Risk Reference Model is already quite ambitious. Specifying relations between risk causes and effects according to the four proposed aspects already requires a sophisticated information and risk management of the company under consideration. The identification of the various elements could be operated especially for SOA, e.g., by analyzing BPEL (Business Process Execution Language) files, service repository, service registry, and routing tables of an Enterprise Service Bus (ESB), WSDL (Web Service Description Language) documents, or code of single web services. Furthermore, if available, the integration of an IT configuration management database might support an automated modeling of existing cause-effect relations and its changes. For identifying relevant vulnerabilities, information from IT security management or from public vulnerability databases (e.g. CVSS) as well as internal databases and documentations can be used (Sackmann, Lowis and Kittel, 2009). Therefore, the IT Risk Reference Model is seen as a novel way to structure the relations between causes and effects of risk that is more accurate than a simple correlation coefficient but still operational. It is an open model that can be extended with new elements and relations, e.g. if new activities in the business project are introduced, new IT services are integrated into the business process, new vulnerabilities are detected, or new threats become known. Thus, it can provide a first concept to a risk manager for aligning information management of a company and to also improve the assessment of the actual IT risk situation. If more detailed data is available, it will facilitate a more detailed modeling than proposed in this contribution.

The relations between the different aspects 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 BP x AP, between the IT applications and the vulnerabilities with the matrix AP x VN, and between the vulnerabilities and the threats with the matrix VN x TH. Applying the IT Risk Reference Model to a company's business processes and IT support requires an additional concept to define how the relations between the elements are formally modeled. Certainly the simplest approach to define, e.g., the relation $l_{i,j}$ between the business process activity BP_i and the IT application AP_j is to model them in a binary manner as:

(5) $l_{i,j} \in \{0,1\} \; \forall \; i \in \{1, \ldots, C\} \wedge j \in \{1, \ldots, D\}$

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". In this manner, the relations between AP and VN elements ($m_{i,j}$) as well as the relations between VN and TH elements ($n_{i,j}$) can also be described. For a short discussion of possible ways to identify the relevant relations, see (Sackmann, 2008b). To keep the model simple and with automated detection and measuring of changes in mind, in this contribution 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. However, if the required data is available, 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 (Alexander, 2003).

For modeling cause-effect relations, the focus is not directed on single relations between elements of different groups but on existing paths, i.e. links between single threats and business processes. Focusing on paths 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. Thus, the fact of patching alone does not necessarily imply a change of IT risk: if the relevant vulnerability is already protected by a security mechanism, the additional patching of the IT application has no further effect. Thus, only changes that also alter the paths between threats (causes) and business processes (effects) have to be taken into consideration. Formally, the sought paths Λ can be calculated as matrix BP x TH by simply multiplying the matrices of the IT Risk Reference Model and normalizing it:

$$(6) \qquad BPxTH = \left[\left(BPxAP \cdot APxVN \cdot VNxTH \right)\right] = \begin{bmatrix} \Lambda_{1,1} & \ldots & \Lambda_{C,1} \\ \ldots & \ldots & \ldots \\ \Lambda_{1,F} & \ldots & \Lambda_{C,F} \end{bmatrix} \qquad \forall\, \Lambda_{c,f} \in \{0,1\}$$

Each path is then characterized by its interlinked elements:

$$(7) \qquad \Lambda_g = \left\{BP_g, AP_g, VN_g, TH_g\right\} \qquad \forall\, g \in \{1, \ldots, G\} \quad \text{with G = number of paths.}$$

FROM HISTORICAL LOSS EVENTS TO AN ADJUSTED LOSS DATABASE

Taking changing cause-effect relations into consideration does not aim at changing the "traditional" IT risk management process – it just opens a new way for building up a more adequate historical loss data base (HLDB) as fundament for the quantification of IT risk by established methods, e.g. by performing a Monte Carlo Simulation to combining the distributions of frequency of loss cases and the distributions of loss amounts.

The basic idea is not only to record, e.g., date, risk category, and monetary loss but to extend the data model of present loss data bases by the actual cause-effect relation that sparked off the loss event. Thus, building up such an extended HLDB would require the identified cause of risk (threat) for each path involved to be recorded as well as the corresponding vulnerability, the IT application, and the business process that have a share in the loss event. Furthermore, a maximal loss, e.g. represented by the value added of the harmed business process, should also be recorded.

The resultant database extends recent historical loss data bases with an explicit assignment of the underlying cause-effect relations for each registered loss event. This allows changes within the IT infrastructure and IT support of business processes to be retraced. As discussed in the following section, an extended HLDB provides a promising starting point to generate a new adjusted loss data base (ALDB) that can be used from existing methods for calculating IT risk reflecting the actual IT situation and, thus, achieving a more accurate assessment of IT risk. For generating such an ALDB that gives information about "what loss would have occurred if the present cause-effect relations had been in place in former times", it is proposed to revaluate each single historical loss event after every change of the cause-effect relations. In the following, a method for the revaluation of historical loss events is proposed. The method contains four phases, i.e. (1) identifying the cause-effect relations of historical loss events and generating the HLDB accordingly, (2) identifying changes of the cause-effect relations and categorizing new paths, (3) assessing the new paths, and (4) transforming the HLDB into the ALDB. These four phases are presented and discussed in the following. For a better understanding, the modus operandi is demonstrated using a hypothetical example.

Phase 1: Generating the HLDB

The first phase requires the identification of all historical known paths within the actual cause-effect relations that are under evaluation. Assuming a simplified company consisting of merely three business processes that are realized by three services having two known vulnerabilities which can be attacked by two types of threats as illustrated on the left hand side of Figure 2.

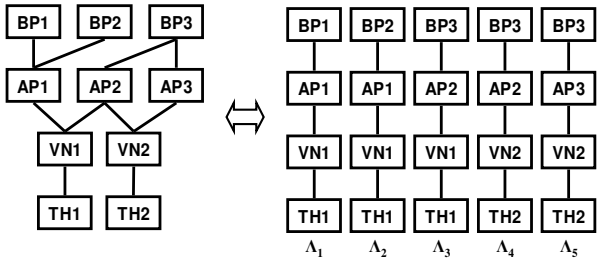

Figure 2: Example of cause-effect relations and paths

In total, five paths can be identified and the respective HLDB is filled with relevant loss events. An extract of an exemplified HLDB is shown in Table 1.

			Path Components				Value	
Date	Time	Path (g)	TH	VN	AP	BP	Added	Loss
21.11.	14:30	1	1	1	1	1	3500	380
		2	1	1	1	2	9000	2160
		3	1	1	2	3	6500	3200
	17:54	4	2	2	2	3	7500	1200
		5	2	2	3	3	7500	1200
22.11.	09:12	4	2	2	2	3	12000	4900
		5	2	2	3	3	12000	4900
	13:47	1	1	1	1	1	3200	1200
		2	1	1	1	2	3000	1900
		3	1	1	2	3	8700	3970
	14:58	4	2	2	2	3	7700	3850
		5	2	2	3	3	7700	3850
	19:19	1	1	1	1	1	2900	750
		2	1	1	1	2	4000	3200
		3	1	1	2	3	6000	3400
24.11.	18:46	1	1	1	1	1	3400	1260
		2	1	1	1	2	13000	5090
		3	1	1	2	3	4000	1700
25.11.	11:13	4	2	2	2	3	7000	980
		5	2	2	3	3	7000	980
27.11.	14:58	4	2	2	2	3	8900	3380
		5	2	2	3	3	8900	3380

Table 1: Example of an extended historic loss database (HLDB)

For calculating the relative loss factor, it is assumed that the maximal loss that could occur is given by the value added of the instance of the business process under consideration. From a business perspective, this assumption might be unrealistic; however, it can be replaced by any other value representing a maximal loss of a business process instance. A further point to be discussed in future work is the splitting of individual loss events in the case where more than one path is responsible. If there are, e.g., two paths between one threat and one business process (like the paths Λ_4 and Λ_5 between the threat TH_2 and the business process BP_3 in Figure 2), it is necessary to split the occurred loss and to assign for each path a corresponding share. In our example, this is done by equal proportions (see Table 1).

Phase 2: Identification and Categorization of New Paths

If time elapses, changes of the cause-effect relations are possible. As described in phase 1, the paths of a new situation have to be identified. All identified paths then have to be analyzed as to whether they are "known" paths, i.e. whether recorded events within the HLDB already exist that have the identical path. If there is a "new" path, corresponding historical data for assessing risk is lacking and a method for estimating the resulting IT risk is required.

Although there are no directly corresponding and already quantified loss events existing for new paths, the HLDB indirectly provides a rich source for estimating the effects of the new path on IT risk. For identifying the most relevant data within the HLDB, it has been proposed to analyze similarities of paths. Following this concept, we suggest to define similarity of paths for the present according to the set of elements Ψ_g two paths have in common. Assuming that two paths with three identical elements are more similar than two paths with only two identical elements and that two paths with two identical elements are more similar than two paths with only one identical element, three types of similarity can be distinguished. It is further assumed that two paths which have identical elements of directly related layers, e.g. between BP and AP or AP and VN, are more similar than two paths that have identical elements of not directly linked elements, e.g. between BP and VN or AP and TH. Making this difference leads to the following five categories of similarity (visualized in Figure 3):

- Similarity of Type I between two paths Λ_a and Λ_b is given when three identical elements exist.

  (8) Type Ia: $\Psi^g = \{BP_g, AP_g, VN_g\} \vee \Psi^g = \{AP_g, VN_g, TH_g\} \wedge \Psi^g \in \Lambda_a \wedge \Psi^g \in \Lambda_b$

  (9) Type Ib: $\Psi^g = \{BP_g, AP_g, TH_g\} \vee \Psi^g = \{BP_g, VN_g, TH_g\} \wedge \Psi^g \in \Lambda_a \wedge \Psi^g \in \Lambda_b$

- Similarity of Type II between two paths Λ_a and Λ_b is given when two identical elements exist.
  (10) Type IIa: $\Psi^g = \{BP_g, AP_g\} \vee \Psi^g = \{AP_g, VN_g\}_b \vee \Psi^g = \{VN_g, TH_g\} \wedge \Psi^g \in \Lambda_a \wedge \Psi^g \in \Lambda$
  (11) Type IIb: $\Psi^g = \{BP_g, VN_g\} \vee \Psi^g = \{AP_g, TH_g\} \vee \Psi^g = \{BP^g, TH^g\} \wedge \Psi^g \in \Lambda_a \wedge \Psi^g \in \Lambda_b$
- Similarity of Type III between two paths Λ_a and Λ_b is given when only one identical element exists and is formally described as follows:
  (12) Type III: $BP_a = BP_b$ or $AP_a = AP_b$ or $VN_a = VN_b$ or $TH_a = TH_b$

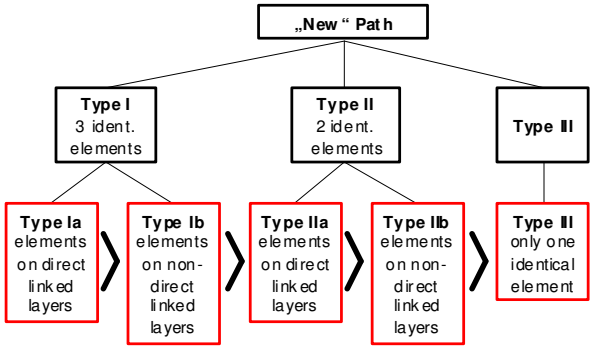

Figure 3: Categories of similarity of two paths

Reverting again to the exemplified company, a change in the prevailing applying cause-effect relations is assumed (Figure 4).

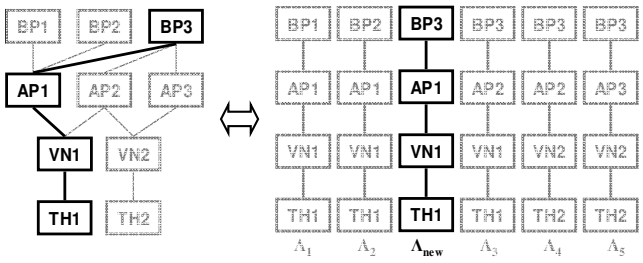

Figure 4: Example of changed cause-effect relations and corresponding new

A new connection between BP_3 and AP_1 occurs and so a new path Λ_{new} evolves. Using the categorization already introduced, two paths can be found in the HLDB which have three elements from directly linked layers in common (Λ_1 and Λ_2). So the new path is of type Ia (Figure 5).

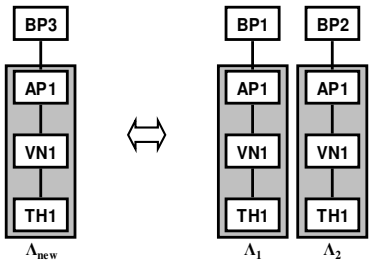

Figure 5: New path with similarity of type Ia

Phase 3: Assessment of New Paths

In the third phase, identified new paths within the cause-effect relations are valuated. All loss events of the HLDB that had been identified as being similar to a new path Λ_{new} are used as basis for this valuation. Since the effect of a loss event is limited in its general validity, it is proposed to use relative instead of absolute loss. Therefore, for any loss event, a relative loss RL is calculated as follows:

$$RL = \frac{Loss}{Value\ Added} \tag{13}$$

To determine the relative loss of the a path $RL(\Lambda_{new})$, the arithmetic mean of all relevant similar paths Λ_k's loss events within the HLSB is calculated as follows:

$$RL(\Lambda_{new}) = \sum_{k=1}^{K} \frac{Rl(\Lambda_k)}{K} \quad \text{with} \quad RL(\Lambda_k) = \sum_{q_k=1}^{Q_k} \frac{RL(\Lambda_{k,q_k})}{Q_k} \tag{14}$$

with K = number of different relevant paths Λ_k within HLDB that are of identified similarity to Λ_{new} with $k = 1,\ldots, K$

Q_k = number of loss events an underlying path Λ_k has within HLDB with q_k as the order number of the relevant loss events with $q_k = 1,\ldots,Q_k$

$RL(\Lambda_{k,q_k})$ = Relative loss of loss event q_k of path Λ_k within HLDB.

$$Q_k = \sum_{k=1}^{K} Q_k > 0 \tag{15}$$

To explain in more detail, the business processes of the exemplary company from above are again reverted to. The new path Λ_{new} (Type Ia) has two similar paths within the HLDB ($K = 2$), namely Λ_1 and Λ_2. For path Λ_1, four loss events within the HLDB ($Q_1 = 4$) as well as for Λ_2 ($Q_2 = 4$) can be found. For calculating $RL(\Lambda_{new})$ formula (14) results in the following:

$$RL(\Lambda_{new}) = \frac{RL(\Lambda_1) + RL(\Lambda_2)}{2} = \frac{0.28 + 0.52}{2} = 0.4 \tag{16}$$

with

$RL(\Lambda_k, q_k)$	$q_k = 1$	$q_k = 2$	$q_k = 3$	$q_k = 4$
Λ_1	0.11	0.38	0.26	0.37
Λ_2	0.24	0.63	0.80	0.39

Table 2: Relative losses of the relevant paths

Phase 4: Filling up the ALDB

In the fourth phase, the aspired ALDB is created containing "new" loss events representing the actual cause-effect relations within the IT supported business processes and provides an adjusted data basis for risk calculation methods. For generating the ALDB, in a first step, all recorded loss events of the HLDB that are existent and have unchanged cause-effect relations are directly copied to the ALDB. This is necessary, since an identical attack is expected to result in an identical loss. All historical loss events whose cause-effect relations are no longer existent, e.g. because a vulnerability has been patched, will not appear in the ALDB. Not only the absolute loss amount is transferred to the ALDB, but also the calculated relative loss for each single path as explained in phase 2. In a second step, anywhere a threat is found that is also relevant for a new path, the ALDB is extended by a corresponding row, showing the new cause-effect relation. The applying loss has to be calculated by multiplying the estimated RL (section 3.3) with the corresponding value added of the relevant business process.

In Table 3, this is demonstrated reviving the example from above: most loss events (not shaded) are direct copies of loss events of the HLDB. Further the ALDB is extended by the corresponding loss events of the new path (shaded) whenever

threat 1 appears. For estimating the absolute loss that the occurrence of threat 1 would have had if path Λ_{new} had already been in place at the moment of occurrence, the expected loss is calculated by multiplying the respective value added of the business process concerned (BP_3) with the calculated average relative loss of the new path (here 0.4). In a further check, it has to be guaranteed that the accumulated RL affecting a single business process at one time cannot exceed 1.

Date	Time	Path No. (g)	TH	VN	AP	BP	Value Added	Loss	RL
21.11.	14:30	1	1	1	1	1	3500	380	0,11
		2	1	1	1	2	9000	2160	0,24
		3	1	1	2	3	6500	3200	0,49
		new	1	1	1	3	6500	2600	0,40
	17:54	4	2	2	2	3	7500	1200	0,16
		5	2	2	3	3	7500	1200	0,16
22.11.	09:12	4	2	2	2	3	12000	4900	0,41
		5	2	2	3	3	12000	4900	0,41
	13:47	1	1	1	1	1	3200	1200	0,38
		2	1	1	1	2	3000	1900	0,63
		3	1	1	2	3	8700	3970	0,46
		new	1	1	1	3	8700	3480	0,40
	14:58	4	2	2	2	3	7700	3850	0,50
		5	2	2	3	3	7700	3850	0,50
	19:19	1	1	1	1	1	2900	750	0,26
		2	1	1	1	2	4000	3200	0,80
		3	1	1	2	3	6000	3400	0,57
		new	1	1	1	3	6000	2400	0,40
24.11.	18:46	1	1	1	1	1	3400	1260	0,37
		2	1	1	1	2	13000	5090	0,39
		3	1	1	2	3	4000	1700	0,43
		new	1	1	1	3	4000	1600	0,40
25.11.	11:13	4	2	2	2	3	7000	980	0,14
		5	2	2	3	3	7000	980	0,14
27.11.	14:58	4	2	2	2	3	8900	3380	0,38
		5	2	2	3	3	8900	3380	0,38

Table 3: Example of an adapted loss data base (ALDB)

Of course, this is only a first and possibly not yet adequate approach to estimate the monetary effect and is still subject to improvement. A more adequate method to obtain this value might improve the estimation results, however it would not change the approach presented in general. Thus, the ALDB reflects – according to the actual new situation – to some degree historic loss events and to another revaluated loss events according to the new cause-effect relations. Such an ALDB is expected to provide a more accurate database due to the actual cause-effect relations and thus improve the precision of IT risk quantification and hence the management of IT risk.

Discussion and Limitations

The approach presented in this contribution provides a first systematic approach to taking fast-changing cause-effect relations in dynamically IT-supported business processes into consideration when assessing IT risk. Since one main focus lies on the applicability of the approach and its implementation in real information systems, there are several trade-offs with accuracy. It provides a systematic approach rather than a finished model and thus involves limitations of considerable importance.

From a business view, the value added of a single (part of a) business process to determine the maximal amount of loss a loss event could cause is proposed in this contribution. Although this measure can be derived relatively easily from controlling systems, it might not necessarily be the best measure. Of course, the fix amount could be replaced from instance to instance by actual amounts and the method for estimating the expected loss of new paths extended accordingly. Alternatively, other values, such as transaction volume in a purchase process as well as a more differentiated view on loss, e.g. direct versus indirect losses, could be taken into consideration. Such modifications would not change the underlying approach of backward-oriented assessment presented here. However, they are seen as valuable information and should be analyzed according to their improvement of risk assessment. A further assessing issue occurs in the case of complex cause-effect relations, i.e. when a loss event is aligned to more than one single path. In this case, since in our approach it is proposed to record loss events according to the paths involved instead of recording the loss event in total, a method is required that allows the total loss amount to be divided amongst the paths involved. An objective method to do so is still subject to further research.

A second limitation is the fact that only elements of the modeled cause-effect relations can be taken into consideration having been involved in a historical loss event at least once. New or formerly unknown elements can be integrated. However, they have to be assessed in an alternative way, e.g. by expert estimations.

A third limitation can be found within the historical loss database itself. In a historical loss database, usually only those events are recorded that finally result in a (financial) loss. This might cause a bias, since threats that had been realized but not resulted in a financial loss are not recorded. If a changed cause-effect relation leads to a previous threat becoming relevant, the loss events belonging to the threat cannot be taken into consideration. To solve this problem, it would be necessary to also record all those events in the historical loss database that are caused by a known threat, irrespective of whether it resulted in a loss or not. Alternatively, the likelihood of loss events could be derived from external data or expert estimation. However, this would require manual adjustment of historical data and go against the aimed automation of risk revaluation.

From an IT security view, attacks that exploit different vulnerabilities in combination are of high practical relevance. Such attacks cannot be modeled by using the IT Risk Reference Model directly. For taking combined attacks into consideration too, it is therefore proposed to interpret them as independent threats and thus to indirectly integrate them into the IT Risk Reference Model.

Although taking cause-effect relations into consideration seems a plausible way to improve risk assessment, the next outstanding step is a proof of concept and an empirical evaluation of the presented approach. While the first is the subject of a current research project, the latter requires an extended database with historical loss events for several periods according to the HLDB presented in section 3. Therefore, in the next step, a first evaluation will be made by simulation tools and by comparing the results with common overall adjustment methods. Irrespective of the results, it seems advisable to any company with highly integrated information systems and/or building up flexible technologies such as service-oriented architectures to think about measuring risk and to build up a well-documented and expressive loss database. Taking account of the flexible cause-effect relations and integrating information about them into the whole risk management process seems a viable proposition. This is an open research field. However, the approach presented in this paper might serve as a good starting point.

REFERENCES

1. Alexander, C. (2003): Managing Operational Risks with Bayesian Networks, in Alexander, C. (Eds.) Operational Risk: Regulation, Analysis and Management. Prentice Hall, London
2. Alter, S., Sherer, S.A. (2004): A general, but readily adaptable model of information system risk, *Communications of the Association for Information Systems* (14), pp. 1-28
3. Blakely, B., McDermott, E., Geer, D. (2001): Information Security is Information Risk Management, in *Proceedings of the New Security Paradigms Workshop 2001*, Cloudcroft, New Mexico, USA, pp. 97-104
4. Brynjolfsson, E., Hitt, L.M. (1998): Beyond the Productivity Paradox. Computers are the Catalyst for Bigger Changes, *Communications of the ACM* 41(8), pp. 49-55
5. BSI - Federal Office for Information Security (2005): IT-Grundschutz Manual, available at URL: https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/intl/intl.html (2010-02-27)
6. Denning, P. J. (1997): A New Social Contract for Research, *Communications of the ACM* 40(2), pp. 132-134
7. Ellis, C.A. (1999): Workflow Technology, in: Beaudouin-Lafon, M. (Ed.): Computer supported co-operative work, Chichester: Wiley, pp. 29-54
8. Faisst, U., Prokein, O. (2008): Management of security risks - a controlling model for banking companies, in Seese, D., Schlottmann, F., Weinhardt, C. (eds.): *Handbook on Information Technology in Finance*, pp. 73-94, Springer, Heidelberg
9. Giaglis, G.M. (2001): A taxonomy of business process modelling and information systems modelling techniques, *International Journal of Flexible Manufacturing Systems* 13(2), pp. 209-228
10. Gordon, L.A., Loeb, M.P. (2002): The Economics of Information Security Investment, *ACM Transactions on Information and System Security* 5(4), pp. 438-457
11. Hayes, B. (2008): Cloud Computing, *Communications of the ACM* 51(7), pp. 9-11
12. Hechenblaikner, A. (2006): Operational Risk in Banken. Eine methodenkritische Analyse der Messung von IT-Risiken, Wiesbaden: DUV (in German)
13. Hevner, A.R., March, S.T., Park, J., Ram, S. (2004): Design Science in Information Systems Research, *MIS Quarterly* 28(1), pp. 75-105.
14. Holton, G.A. (2003): Value-at-Risk: Theory and Practice, Academic Press, San Diego
15. Jaisingh, J., Rees, J. (2001): Value at risk: A methodology for information security risk assessment, *Proceedings of the INFORMS Conference on Information Systems and Technology 2001*, Miami

16. Krafzig, D., Banke, K., Slama, D. (2005): Enterprise SOA. Prentice Hall, Upper Saddle River
17. McAfee, A., Brynjolfsson, E. (2008): Investing in the IT that makes a competitive Difference, *Harvard Business Review*, July-August 2008, pp. 2-10
18. McNeil, A., Frey, R., Embrechts, P. (2005): Quantitative Risk Management: Concepts Techniques and Tools. Princeton University Press, Princeton
19. Mercuri, R.T. (2003): Analyzing Security Costs, *Communications of the ACM* 46(6), pp. 15-18
20. Mills, S. (2007): The future of business – Aligning business and IT to create an enduring impact on industry, *IBM Thought leadership paper*, available at URL: ftp://ftp.software.ibm.com/software/soa/pdf/future_of_business.pdf (2010-02-17)
21. Muehlen, M., Rosemann, M. (2005): Integrating Risks in Business Process Models, *Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005)*, Sydney
22. Parker, D.B. (2007): Risks of risk-based security, *Communications of the ACM* 50(3), p. 120
23. Rörig, S. (2007): Using Process Models to Analyse IT Security Requirements. Thesis, University of Zurich
24. Sackmann, S. (2008a): Assessing the effects of IT changes on IT risk – A business process-oriented view, in *Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI'08)*, Munich, pp. 1137-1148
25. Sackmann, S. (2008b): A Reference Model for Process-oriented IT Risk management, in *Proceedings of the 16th European Conference on Information Systems (ECIS'08)*, Galway
26. Sackmann, S., Lowis, L., Kittel, K. (2009): Selecting Services in Business Process Execution – A Risk-based Approach, in Hansen, H.R. et al. (Eds.): Business Services: Konzepte, Technologien, Anwendungen, 9. Internationale Tagung Wirtschaftsinformatik, Wien: Österreichische Computer Gesellschaft (246), pp. 357-366
27. Sanchez, R. (1995): Strategic Flexibility in Product Competition, *Strategic Management Journal*, 16, Special Issue: Technological Transformation and the New Competitive Landscape, pp. 135-159
28. Salvati, D., Diergardt, M. (2007): Towards a Scenario Based Risk Model for Information Systems. Laboratory for Safety Analysis. ETH Zurich, Zürich, available at URL: http://www.lsa.ethz.ch/people/phd/salvatid/DS-Scenario-Based-Risk-Model.pdf (2008-09-29)
29. Scheer, A. W. (2000): ARIS - Business Process Modeling. Springer, Berlin
30. Tsichritzis, D. (1998): The Dynamics of Innovation," in Beyond Calculation: The Next Fifty Years of Computing, New York: Copernicus Books, pp. 259-265