IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5206

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

A Model to Enhance Risk Management of IT-Supported Business Processes

Christian Otto and Claus Rautenstrauch

Otto-von-Guericke-Universität Magdeburg, Dept of Business Info. Systems (FIN/ITI), PO Box 4120, D-39106 Magdeburg, Germany

otto@iti.cs.uni-magdeburg.de

ABSTRACT

KonTraG and Basel II explicitly require enterprises to implement a risk management system including a forewarn function. Monitoring systems for technical infrastructure deliver basic data in the sense of this function, that can be used for IT-risk management. Yet, this data has to be processed and selected appropriately, in order to be applied for usage as risk indicators in a risk management system. On the basis of system monitoring this paper introduces a bottom-up approach, on which an IT-risk management system can be implemented.

INTRODUCTION

On May 1, 1998 a new German law called KonTraG became effective. The law was the response of the German legislator to numerous insolvencies worldwide, enforcing German executives´ responsibility to take care of an adequate risk management system (BMJ 1997). Without defining specifically, how the risk management system should be designed, the minimum requirement is that risks are identified early enough, so action can be taken to avoid impending bankruptcy.

Additionally, the risk management discussion is intensified through Basel II.

Basel II, an internationally accepted board to develop directives for the banking industry, currently reforms the directives of risk provision. Therefore, banks will have to go beyond the perspective of credit risks, adding operative risks to the risk management portfolio (Basel II 2003, p. 10). Operative risks are defined as risks due to inadequacy or failure of internal procedures, human error, system breakdown or external events (Basel II 2003, p. 10). The basis to this paper is the assumption, that the methods for treatment of operative risks will develop rapidly (Basel II 2003, p. 10).

Due to the common use of information systems to support business processes it becomes apparent that business informatics can contribute to the Basel II motivated discussion about treatment of operational risk. Since enterprises are increasingly dependent upon their technical information infrastructure, it is the task of business informatics to deliver the part of a risk management system which deals with accompanying IT-risks.

FROM RISK TO RISK MANAGEMENT

Objective and Risk Dimensions

The term risk is defined diversely in literature (Wolf et al. 2001, p.22 et seq.). A common classification differentiates extensive-, decision- and information oriented definitions (Imboden 1983, p. 41). The extensive definitions see risk as the possible failure of an effort. Decision oriented definitions focus on whether a wrong decision imposes a risk to an enterprise, while information based approaches postulate that uncertainty, indeterminacy and incompleteness are responsible for arising risks.

Extensive risk definitions serve as a basis for further examinations of the correlation between IT-risk indicators and the business processes supported by information systems. *Zellmer* defines risk as the possibility of not achieving objectives and such gives an apparent example of an extensive risk definition (Zellmer 1990, p. 12). The correlation between objectives and risks is visualized in fig. 1.

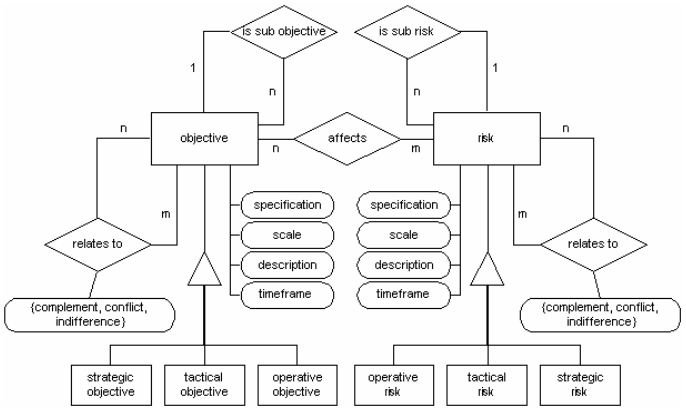
Derived from the concept of the management pyramid (Horvath 1982, p. 368), the entrepreneurial objectives can be divided into strategic-, tactical- and operative ones. Strategic goals are of middle- and long term orientation, are of little detail and form the superior objectives of an enterprise. Tactical objectives are of middle- through short term orientation and provide a more detailed perspective (Staehle 1990, p. 72), whereas operative objectives give short term, specific and detailed instructions. It becomes apparent, that subordinate objectives help to achieve the superior objectives (Braun et al. 1999, p. 233). Objectives standing on the same level come in conflict or stand in complementary- or indifferent relation to one another.

The correlation between objectives and risks is shown in fig. 1 and can be marked as symmetric in structure. Viewed as reversed image, the strategic-, tactical- and operative objectives are endangered by the corresponding risk dimensions.

Strategies dealing with risks and their impacts respectively, can be of preventive or reactive nature. The earlier actions to cope with risks are taken, the lower is the effort needed to smooth a loss and the more options remain to influence the risk potential (BME 2000, p. 8). The concept of the risk reduction stairway categorizes the strategies (Gaulke 2000, p. 68 et seq.):

Risk prevention means to avoid or to reduce activity to a minimum that carries a risk potential. Risk reduction tries to lower the likelihood of a damage or loss in terms of preventive steps. Risk restriction caps the possible impact of a loss. By insuring a risk or by outsourcing a service,

Figure 1. Symmetry Between Objectives and Risks



risk is being relocated. The final strategy is to take on all residing risks in the cases, where they do not impose an existential risk to the enterprise.

These strategies require that risks are known and weighted in accordance with their loss potential, so that preventive action is being coordinated in a balanced cost-/benefit ratio. Finally, adequate indicators have to be assigned in order to be able to early identify the risk potential. Business sciences summarize the steps of risk identification, measurement and treatment in a risk management circuit. The following section introduces selective steps within the risk management circuit, so the model to follow can be appropriately classified.

Selective Parts of the Risk Management Circuit

Risk Identification

The aim of the risk identification step is to detect risks completely, quickly and at an early stage (Zellmer 1990, p. 26 et seq.). Additionally, risk identification has to be aligned with the objectives of an enterprise (KPMG 2000, p. 21). The specification, scale, description and timeframe more specifically describe an objective (see fig. 1). The individual dimension of an objective is opposed by a corresponding risk dimension (see fig. 1). If the dimensions, risk and objective are inscribed into a matrix, an overview is given which entrepreneurial objective is endangered by which risk (see fig. 2).

Risk Treatment with Indicators

The main task of risk controlling is to supply management information on present and potential risk (Lück 1998, p. 1929). By appointing indicators to risks, the task of alerting risk management in advance can be accomplished (Schmitting et al. 2003, p. 537).

The relation between risk and indicator is suggested to be a 1:n relation (Schmitting 2003, p. 534). Thus, each risk may have one or more indicators. If more than one indicator is appointed to a risk this constellation is called indicator bundling. Within IT, n:m relationships between risks and indicators seem apparent, i.e., through indicator bundling one indicator is suitable for monitoring several risks.

Indicators have to meet certain quality criteria, which are summarized in fig. 3. In addition, indicators have to be valid and reliable, demanding that they firstly measure the right values and secondly do so in an accurate manner.

In order to be able to efficiently control risks, a target value and a corresponding tolerance has to be assigned to an indicator. This proceeding is derived from the controlling circuit (Horvath 1998, p. 12), where target and actual values are analyzed. If the actual value leaves the permitted corridor, action has to be taken to bring the system back onto path (Kütz 2003, p. 2 et seq.).

Taking indicator bundling into consideration, the tolerated bandwidth has to be defined for the combination of different indicators. The limit can be exceeded if one, the majority or all indicators measure a critical value.

Figure 2. Objective/Risk Matrix

	objective 1:	objective 2:	…	objective n:
risk 1:	$E(R_1)$	$E(R_1)$	...	
risk 2:		$E(R_2)$	…	$E(R_2)$
...	...	...	...	...
risk n:	$E(R_n)$	$E(R_n)$	…	
$\sum$	$\sum_1^n (R_n)$	$\sum_1^n (R_n)$	$\sum_1^n (R_n)$	$\sum_1^n (R_n)$

Figure 3. Indicator Quality Criteria (s1: Bitz 2003, p. 54 et seq., s2: Krystek et al. 1993, p. 103 et seq.)

requirement	description
uniqueness	room for misinterpretation should be eliminated (s1).
completeness	the monitored domain should be covered completely (s1).
earliness	time has to be sufficient to react upon an indicated alert (s1).
early availability	the indicator has to be contemporarily available (s2).
economical tenability	the effort needed to supply the indicator need to be in reasonable cost-/benefit relationship (s1).
stability	the displayed relationships must be robust, meaning that also discontinuous trends can be integrated (s2).
sensibility	lower stages of aggregation are to be preferred so earliness can be kept up (s2).
descriptiveness	the relationships have to be comprehensible (s2).
flexibility	despite stability, adjustments have to be possible (s2).

Having focused on the general risk management process so far, the perspective is narrowed in order to explore, if IT-indicators derived from the monitoring of base and application systems are suitable for controlling IT-supported business processes. Basel II defines IT-risks being part of operative risks (see fig. 1). Thus, the next section will pick up the basics of IT-monitoring in order to be able to build a model for the risk management of IT-supported business processes.

IT-MONITORING SUPPLYING INDICATORS

Monitoring Concept and Objective

Risk identification and treatment are the steps from the risk management circuit, to which monitoring of IT-systems can be assigned. Detecting critical system behavior in advance require for specific signaling indicators (Zimmermann 2003, p. 10). The increasing complexity demands to make use of monitoring tools, i.e., software which assists in monitoring the information systems.

Monitoring Characteristics

Monitoring methods can be separated into real-time and historical methods. Real-time monitoring, which is also referred to as event/fault monitoring, reports actual states. Service or system failure can be detected and reported (Clauß et al. 2003, p. 247). Historical monitoring generates statistics of system characteristics, like availability, utilization and operational capacity (Clauß et al. 2003, p. 246). A special form of real-time monitoring is the so called approximate real-time monitoring. The object is not being observed continually, but in certain time intervals (Zimmermann 2003, p. 11). This method is of advantage, if the observed object changes slowly over time.

Monitoring Objects

Hardware, software and networks are three object categories to be monitored. Hardware is commonly separated into the central processor unit (cpu), the memory, internal connections, I/O-devices and periphery. If one of the three first mentioned hardware components fails, a system break-down may be the consequence. Thus, real-time monitoring seems appropriate for these system parts. Failure within the other mentioned components may lead to disturbance of system performance (Zimmermann 2003, p. 17 et seq.). Fig. 4 gives an overview which criteria apply to supervise hardware components (Zimmermann 2003, p. 181).

In order to ensure smoothly running system processes, besides hardware, also software has to be monitored. Fig. 5 gives an overview of monitoring criteria. Within network components (i.e. switches, routers) software and hardware is closely linked. Network monitoring focuses on availability, connectivity and efficiency.

Figure 4. Hardware Monitoring Criteria

category	example of criteria
1. CPU	availability efficiency
2. memory	efficiency correctness of saved data
3. internal connectivity	I/O-queues of busses correctness of transmitted data
4. I/O-devices	availability efficiency
5. periphery	temperature humidity current entry

Figure 5. Software Monitoring Criteria

criteria	description
availability	timeframe of software usability
CPU-load	timeframe during which software uses the CPU
memory load	timeframe and extent of memory usage
user	timeframe and number of users
storage – capacity	extent of hard disk usage through software
I/O – utilization rate	access frequency of I/O - devices

Controlling Business Process IT-Risks

Within in the scope of analyzing monitoring data, the question about legitimacy of this bottom-up approach within risk management arises, immediately. However, legitimacy becomes apparent by taking a closer look at an enterprise, from the perspective of business informatics. Controlling of IT-supported business processes consequently finds its beginning within monitoring of base systems (Rautenstrauch et al 2003, p. 6), which are the platform for any following application. If the base systems are not ready for service, the applications will not be either. Therefore, the gap between IT-supported business processes and the service delivering base systems has to be bridged. This task can be managed by the suggested model, using quality contact points between user and IT-system, which were firstly discussed by *Wall* (Wall 1997, p. 107).

DRILL-DOWN FROM THE BUSINESS PROCESS TO THE IT-SYSTEM

Identification of IT-Risks in Business Processes

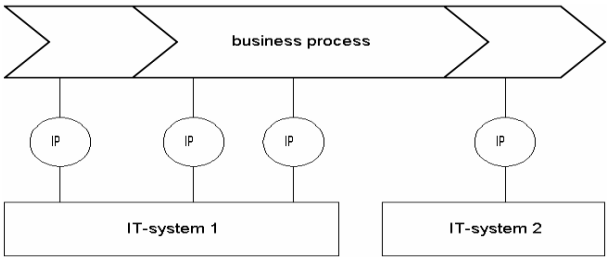
Constructing a Tree-Layer-Model

The relationship between a business process and the underlying IT-landscape can be visualized in a three-layer-modell (see fig. 6).

The first layer represents the business processes to be controlled. On this layer the process is being recorded, decoupled from the underlying IT-system. An intermediate layer houses the interaction points (IP) between the business processes and the information technology. The interaction point may be an entry mask or the display of a calculated result, for instance. The performance of the IT-system is actively recognized by the employee involved in the process in that interaction point. The bottom layer represents the components of the information infrastructure, which is needed to support the business process.

On the interaction layer several kinds of interactions can be distinguished. Firstly, interaction in terms of a human machine interface becomes apparent. Furthermore, the users can be separated into external

Figure 6. Three-Layer-Model



(i.e. customers) and internal (i.e. employees) ones. Secondly, even if using an automatic interface, the interaction point between business process and IT-system still serves as a quality measuring point.

Interaction Tolerance

In the case of a human machine interface the users may be differentiated into interaction tolerant and intolerant ones. The group of interaction tolerant users may consist of employees, who, in case of a problem, are supported by a user help desk. Interaction intolerant users may be customers, who, due to their independence, are free to select their preferred enterprise or service and thus the supporting IT-system.

Using automatic interfaces does not immediately lead to human quality perception in the interaction point. The perception will take place in the next interaction point of a human machine interface. Consequently, the automatic interfaces and their interaction point remain in focus, since the intended controlling of business process functionality via IT-indicators provides adequate data measuring interface functionality.

Quality Perception

The quality of a supportive service is noticed by the user who uses an IT-system within a work process in the interaction point. Interaction points are also referred to as contact points between the user being looked at as a customer and the IT-system as a service provider (Wall 1997, p.101). The quality perception of the user is determined as the sum of the performance being measured in the interaction points.

Measurement of IT-Risks in Business Processes

Regarding IT-supported business processes, three categories describing functionality lie on hand:

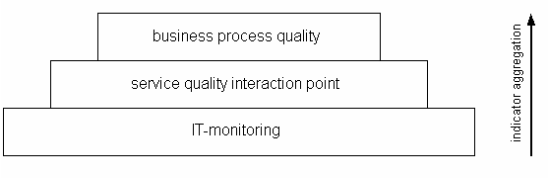
- *Unrestricted functionality:* all tasks within the process are fully supported. In terms of time and factual matters no restrictions apply.
- *Restricted functionality:* the process is not fully supported. Some restrictions apply, though, the process is still supported with limited comfort. Comfort can be restricted on the time and factual scale, leading either to a slower processing velocity or to inadequate results, calling for a workaround solution.
- *Failure of functionality:* the process is no longer supported by the IT-system. In time and factual matter no alternatives apply.

The described categories of possible malfunction, constitute a risk. This risk has to be controlled using data derived from IT-monitoring.

Treatment of IT-Risks in Business Processes

As yet, monitoring of single components of the information infrastructure is often carried out. The relevance of the failure for the functionality of the business process remains unnoticed. Thus, there is the risk that a business critical malfunction, in the sense of risk management, is not being taken care of or with inappropriate priority. Therefore, IT-monitoring has to be enhanced as follows:

Figure 7. Indicator Aggregation



Starting with all critical business processes, which have been identified, these processes need to be investigated in respect of its technical support. First, every affected base system has to be determined. The base systems have to be controlled in regard of its functionality, using appropriate indicators. The business process is enabled, if all relevant base systems are ready-to-operate. The relationship between the different layers being looked at, as functionality on the business process-, interaction point- and IT-system layer, is visualized in fig. 7.

The functionality on the IT-system layer is represented by indicators from the IT-monitoring. These indicators allow for statements regarding response time or memory utilization. The indicators referred to are suitable to be used in operative terms.

In the interaction point not only one system is in focus, but all systems which serve in that point. Therefore, the measurement of service-quality is determined as the sum of performance of each single system, affecting the interaction point. The interaction quality is suitable for risk treatment on operating-department level.

The overall IT-service-quality of a business process can be determined as sum of the quality level being measured in all interaction points. This aggregated view can be used in middle- and top management reports, and, is therefore particularly applicable to be used within service level agreements. On this aggregation level communication between service provider and service customer is improved, since the customer in the first place expects information on the quality of its business support and not on data regarding single base systems. In the case of internal IT-production the advantages equally apply to the internal customer/ supplier relationship.

The model shows the opportunity to drill-down from the business process to the underlying base systems. In reverse, the model also allows to ask for, which business process is supported by the regarded base system. Thus, the model allows for translation of IT-risk indicators, in the form of monitoring data, into quality statements concerning the functionality of IT-supported business processes.

CONCLUSION

This bottom-up approach to detect risk indicators on the basis of monitoring data, complies with German legislator's demand for a forewarn function within risk management. Having been an isolated controlling function with all inherent defects, so far, IT-risk management now can be developed as a continuous IT-risk management system. The supported spectrum reaches from an operative alert system to a strategic planning instrument.

It becomes apparent, that data warehouse technology would be suggestive to handle the extensive data extracted from system monitoring. First approaches with conventional data warehouse systems have shown, that they are not adequate for the treatment of monitoring data, since time horizons are relatively short and non-monetary data has to be processed (Zimmermann 2003). Further research and development work is necessary, in order to make use of data warehouse technology for IT-risk management on the basis of monitoring data and risk indicators.

BIBLIOGRAPHY

Basel II: Basler Ausschuss für Bankenaufsicht (2003): Konsultationspapier – Überblick über die Neue Basler Eigenkapitalvereinbarung.

Bitz, H. (2003): Risikomanagement nach KonTraG: Einrichtung von Frühwarnsystemen zur Effizienzsteigerung und Vermeidung persönlicher Haftung. Stuttgart.

BME: Bundesverband Materialwirtschaft, Einkauf und Logistik e. V. (2000): Risikomanagement in der Beschaffung: Leitfaden für Unternehmen zur Beherrschung der Risiken im Beschaffungsprozess. Frankfurt/M.

BMJ: Bundesministerium der Justiz (1997), Begründung zu § 91 AktG.

Braun, F./Gänger, M./Schmid, P. (1999): Risikomanagement in Versicherungsgesellschaften. In: Saitz et al. (Hrsg.), p. 231-261.

Clauß, M./Müller, T./Ziegler, C./Hübner, U. (2003): Prinzipien der Systemadministration. Vorlesungsskript,TU Chemnitz 2003, http://www.tu-chemnitz.de/urz/lehre/psa/script03/, http://www.tu - chemnitz.de/urz/lehre/psa/script03/8.August 2003.

Gaulke, M. (2000): Risikomanagement bei IT-Projekten, In: KES – Zeitschrift für Kommunikations- und DV-Sicherheit, Ingelheim, Nr. 5/2000, p. 66-68.

Grundel, H. (1997) (Hrsg.): Struktur und Leistungsspektrum innovativer Rechenzentren: Vorträge der 12. GI Fachtagung über Rechenzentren am 19. und 20. Juni 1997 in Stuttgart-Möhringen. Heidelberg.

Horváth, P. (1982): Aufgaben und Möglichkeiten des Controlling in Klein- und Mittelbetrieben. In: Krallmann (1982), p. 360-379.

Horváth, P. (1998): Das Controllingkonzept – Der Weg zu einem wirkungsvollen Controllingsystem. 3. Auflage, München.

Imboden, C. (1983): Risikohandhabung: Ein entscheidungsbezogenes Verfahren. Stuttgart/Bern.

KPMG (2000): Integriertes Risikomanagement. Berlin.

Krallmann, H. (1982) (Hrsg.): Unternehmensplanung und –steuerung in den 80er Jahren: Eine Herausforderung an die Informatik. Anwendergespräch, Hamburg, 24.-25. November 1981. Berlin et al.

Krystek, U./Müller-Stewens G. (1993): Frühaufklärung für Unternehmen – Identifikation und Handhabung zukünftiger Chancen und Bedrohungen. Stuttgart.

Kütz, M. (2003) (Hrsg.): Kennzahlen in der IT – Werkzeuge für Controlling und Management. Heidelberg.

Lück, W. (1998): Der Umgang mit unternehmerischen Risiken durch ein Risikomanagementsystem und durch ein Überwachungssystem. In: Der Betrieb, 51 (1998) 39,
p. 1925-1930.

Rautenstrauch, C./Schulze, T. (2003): Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker. Berlin et al.

Saitz, B./Braun, F. (1999) (Hrsg.): Das Kontroll- und Transparenzgesetz: Herausforderungen und Chancen für das Risikomanagement. Wiesbaden.

Schmitting, W./Siemes, A. (2003): Konzeption eines Risikomanagementmodells: Begriffsrahmen und IT-Umsetzung. In: CM controller magazin, Bd. 6/2003, p. 533-540.

Staehle, W. (1990): Management: eine verhaltenswissenschaftliche Perspektive. 5. Auflage, München.

Wall, F. (1997): Prozessorientiertes Controlling der Dienstleistungsqualität. In: Grundel (1997), p. 97-122.

Wolf, K./Runzheimer B. (2001): Risikomanagement und KonTraG: Konzeption und Implementierung. 3. Auflage, Wiesbaden.

Zellmer, G. (1990): Risiko-Management. Berlin.

Zimmermann, R. (2003): Reporting über Monitoringdaten im ASP-Umfeld mit Hilfe von SAP Business Information Warehouse®. Diplomarbeit, O.-v.-Guericke Universität Magdeburg, Magdeburg.