University of Augsburg
Prof. Dr. Hans Ulrich Buhl
Research Center
Finance & Information Management
Department of Information Systems
Engineering & Financial Management

Discussion Paper WI-170

Management of Security Risks - A Controlling Model for Banking Companies

by

Ulrich Faisst, Oliver Prokein[1]

January 2006

appears in: Schlottmann, F., Seese, D., Weinhardt, C., Handbook on Information Technology in Finance, Springer, Berlin, 2006.

Erweiterte und überarbeitete Fassung des Beitrags WI-152.

[1] Institut für Informatik und Gesellschaft, Universität Freiburg

Management of Security Risks - A Controlling Model for Banking Companies

Ulrich Faisst[1] and Oliver Prokein[2]

[1] Department of Information Systems & Financial Engineering, Business School, University of Augsburg, Germany, email: Ulrich.Faisst@wiwi.uni-augsburg.de

[2] Institute of Computer Science and Social Studies, Department of Telematics, University of Freiburg, Germany, email: Oliver.Prokein@iig.uni-freiburg.de

Summary: Increasing importance of information and communication technologies (ICT), new regulatory obligations (e.g. Basel II) and growing external risks (e.g. hacker attacks) put security risks in the management focus of banking companies. The management has to decide whether to carry security risks or to invest into technical security mechanisms in order to decrease the frequency of events or to invest in insurance policies in order to lower the severity of events. Based on a presentation of the state-of-the-art in the management of security risks, this contribution develops an optimization model to determine the optimal amount to be invested in technical security mechanisms and insurance policies. Furthermore the model considers budget and risk limits as constraints. This article is particularly supposed to help practitioners in controlling security risks.

Annotation: This contribution is an enhanced and revised version of the following already published contribution: Faisst U, Prokein O (2005) An Optimization Model for the Management of Security Risks in Banking Companies. In: Müller G, Lin K-J (eds.) Proceedings of the Seventh IEEE International Conference on E-Commmerce Technology CEC 2005, Munich, IEEE Computer Society Press, Los Alamitos, CA, pp. 266-273

Keywords: Risk Management, Security Risks, Controlling Model, Security Mechanisms, Insurance Policies

Introduction

Increasing virtualization of business processes and the cumulative adoption of ICT involved leverage the importance of security risks. The "Electronic Commerce Enquête IV" inquiry carried out in August 2004 concluded that the majority of German banking companies plan to increase the investments in ICT within the next two years (Sackmann and Strüker 2005).

However, the rising deployment of ICT implicates growing security risks. To lower security risks, banking companies may invest into technical security mechanisms and insurance policies. Generally, the more a banking company invests into technical security mechanisms and insurance policies, the lower are the expected losses and opportunity costs of the economical capital charge, et vice versa (Faisst 2004). Overall, a trade-off exists between the expected losses and the opportunity costs of the economical capital charge on the one hand and the investments in technical security mechanisms and insurance policies on the other.

In practice, such investment decisions depend on explicit responsibilities within a banking company. In case, where an explicit responsibility exists, the decision-maker might tend to make every possible investment within his budget, although holistically viewed not every investment is profitable. If no explicit responsibility exists, the decision-maker might tend to minimize costs and therefore neglects further investments, although such investments are profitable in a holistic view.

This contribution aims at developing an optimization model that is able to map the described trade-off between the expected losses and the opportunity costs of the economical capital charge on the one hand and the investments in security mechanisms and insurance policies on the other in a decision calculation. Moreover, the model helps to allocate available budgets to security mechanisms (ex-ante prevention) and into insurance policies (ex-post risk transfer) in an efficient way.

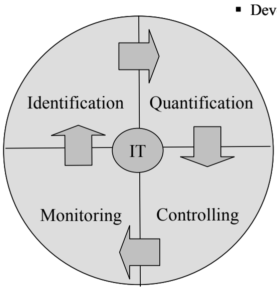
In order to present the state-of-the-art of the management of security risks we will portray the risk management cycle.

The risk management cycle

The following risk management cycle in Fig. 1 illustrates the main activities to handle security risks. The cycle contains four phases: identification, quantification, controlling and monitoring (Piaz 2001).

- Identification of threats
- Classification of security risks, e.g. on base of the concept of multilateral security
- Determination of risk sources and drivers

- Determination of the frequency and severity of events caused by security risks
- Quantification of the aggregated losses in the „average case“
- Development of „worst-case“ scenarios



- Risk reporting (internal & external)
- Early warning systems

- Analysis of measures to prevent risks (ex-ante) and to transfer risks (ex-post)
- Decision support based on necessary investments vs. expected reduction of expected and unexpected losses

Fig. 1. The risk management cycle

Identification Phase

Within the scope of the identification phase the security risks are identified and classified. Security in ICT covers the wide range from the physical protection of the hardware to the protection of personal data against deliberate attacks (Müller et al. 2003). In an open information system like the Internet, one cannot assume, that all parties involved (such as communication partners, services providers etc.) trust or even know each other (Müller and Rannenberg 1999). Therefore, the analysis of security risks requires not only the observation of external attackers but also the inclusion of all parties involved as potential attackers. The concept of multilateral security (Rannenberg 1998) considers the security requirements of all parties involved. The security risks result from the threat of the so-called four protection goals of multilateral security according to Müller and Rannenberg (Müller and Rannenberg 1999):

- Confidentiality,
- Integrity,
- Accountability,
- Availability.

Confidentiality

Firm specific data or personal data of individual users may not be noticed of unauthorized users:

- Message contents have to be confidential in respect of all parties apart from the communication partner,
- communication partners (sender and/or recipients) have to be able to remain in an anonymous way to each other. It should further be possible for other parties to observe them,

- for either potential communication partners or other parties should it be possible to determine the current location of a mobile terminal or its user without his consent.

Integrity
A change of messages by unauthorized people may not be unnoticed, i.e. manipulation of messages must be detected.

Accountability
Accountability of communication transactions is indispensable for a required internalization of actions. Responsibilities and liabilities, efficient incentive scheme, definition of property rights and their transactions are otherwise not to be established:

- The recipient of a message should be able to proof to a third party that a certain communication partner has sent the message,
- the sender of a message should be able to prove and verify the sending of a message together with its actual content. Beyond it, it should be possible for the sender to prove that the message was received,
- the payment for the used services cannot be withheld from the provider – at least the provider receives sufficient evidence that a service was requested. In contrary the service provider can only require payment for services which are correctly provided.

Availability
A restricted availability can lead to material or immaterial impacts, i.e. the communication network has to enable communications between all requiring partners.

The concept of multilateral security is a possible concept to define security risks. Moreover, to quantify the security risks it is necessary to consider the attacks that threat and violence the four protection goals. According to the CSI/FBI Computer Crime and Security Survey (CSI/FBI 2005) viruses, unauthorized attacks and the theft of proprietary information are the most profoundly attacks. Table 1 illustrates the protections goals of multilateral security, selected attacks and potential economic impacts. The probability of loss occurrence arises from the observed attacks, the amount of losses from the economic impacts.

Table 1. Economic impacts of attacks

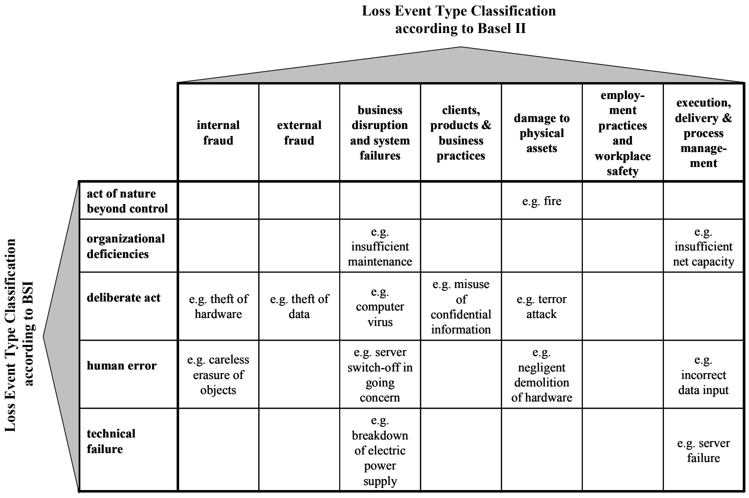
Protection goal	Selected attacks	Potential economic impact
Confidentiality	Theft of data, access misuse etc.	Loss of competitive advantage, liability claims of third, punishments etc.
Integrity	Sabotage, man-in-the-middle-attack, computer bug etc.	Loss of data, business interruption, sales shortfall etc.

Accountability	IP-spoofing, social hacking, inadequate access control etc.	Loss of image, business interruption, liability claims of third etc.
Availability	distributed denial-of-service-attack, computer virus, server failure etc.	Loss of recovery, loss of market share etc.

The threats can be classified into different categories. The German "Bundesamt für Sicherheit in der Informationstechnik (BSI)" differs between the categories act of nature beyond control (e.g. fire), organizational deficiencies (e.g. insufficient maintenance), human error (e.g. incorrect data input), technical failure (e.g. server failure) and deliberate act (e.g. theft of hardware) (BSI 2004).

According to Basel II banks have to charge capital for operational risk. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems of from external events. This definition includes legal risks, but excludes strategic and reputational risk (Basel Committee on Banking Supervision 2001).

Security risks are a subset of operational risks. Fig. 2 provides a comparison of the loss event type classification according to Basel II and the loss event type classification according to BSI, which portrays that security risk are included in a large number of categories of operational risk.



Loss Event Type Classification according to Basel II

Loss Event Type Classification according to BSI

	internal fraud	external fraud	business disruption and system failures	clients, products & business practices	damage to physical assets	employment practices and workplace safety	execution, delivery & process management
act of nature beyond control					e.g. fire		
organizational deficiencies			e.g. insufficient maintenance				e.g. insufficient net capacity
deliberate act	e.g. theft of hardware	e.g. theft of data	e.g. computer virus	e.g. misuse of confidential information	e.g. terror attack		
human error	e.g. careless erasure of objects		e.g. server switch-off in going concern		e.g. negligent demolition of hardware		e.g. incorrect data input
technical failure			e.g. breakdown of electric power supply				e.g. server failure

Fig. 2. Security risks as a subset of operational risks

Quantification Phase

The identified security risks are measured by the use of different methods within the quantification phase (Cruz 2002). So far, no quantification model has been developed for the measurement of the security risks, defined above. For the measurement of this subset of operational risk the Basel Committee on Banking Supervision (Basel Committee on Banking Supervision 2004) suggests five different quantification methods in order to determine the economical capital charge. The methods reach from simple, factor-based approaches to complex stochastic loss distribution models based on the Value-at-Risk (Basel Committee on Banking Supervision 2004). Beyond that, further methods exist for the quantification of operational risks, as for instance questioning techniques or causal methods, like Bayesian Belief Networks (Faisst and Kovacs 2003). Selected methods are described more detailed in the following.

Questioning techniques

Questioning techniques subsume methods like expert interviews and self-assessments by responsible managers. Operational risks are identified and quantified by using structured interview guidelines as well as management workshops. Beside the identification and quantification of operational risks questioning techniques are used to leverage the awareness of operational risk within the company.

Indicator approaches

Indicator approaches use a specific indicator (single indicator approaches) respectively a set of key indicators (key indicator approaches) to indirectly determine the amount of operational risk. Such indicators are selected on base of empirical surveys as well as expert opinions in case the coherence to operational risk can be assumed. An example of the simple indicator approach is the Basic Indicator Approach (Basel Committee on Banking Supervision 2001), on which the gross income of a banking company is used as an exposure indicator multiplied with a factor to determine the economical capital charge. Key indicator approaches consider a set of specific indicators. These comprise key indicators for historic losses, company-specific risk indicators, such as down-time of systems, employee loyalty or the number of transactions. Such indicators may be finally gathered in a scorecard for operational risk.

Stochastic methods

Stochastic methods use distribution functions to describe the level of operational risk. One of these methods is the operational Value-at-Risk. This approach is based on the general Value-at-Risk approach which was originally developed for market risks (Beek and Kaiser 2000). The frequency and severity of events are normally forecasted by proceeding simulations based on historical loss data.

Causal methods

Causal methods are used to analyse the coherence between sources and drivers of operational risk and resulting losses. Such a method is e.g. Bayesian Belief networks. Bayesian Belief networks can be used to connect historical data on past events on the one hand with expert opinions on future events on the other hand.

Table 2 classifies the described quantification methods.

Table 2. Overview on quantification methods[1]

Questioning techniques: ▪ Expert interviews (Piaz 2001) ▪ Self assessments (Piaz 2001)	Indicator approaches: ▪ Single indicator approaches ➢ Basic Indicator approach (Basel Committee on Banking Supervision 2004) ➢ Standardized approach (Basel Committee on Banking Supervision 2004) ➢ Internal measurement approach (Basel Committee on Banking Supervision 2001) ➢ CAPM-approach (Beeck and Kaiser 2000) ▪ Key indicator approaches ➢ Key performance indicator approaches (Piaz 2001) ➢ Key risk indicator approaches (Piaz 2001) ➢ Scorecard approaches (Basel Committee on Banking Supervision 2001)
Stochastic methods: ▪ Loss distribution approach based on operational Value-at-Risk (Basel Committee on Banking Supervision 2001) ▪ Extreme value theory (Cruz 2002)	Causal methods: ▪ Bayesian Belief Networks (Gemela 2001) ▪ Neural Networks (Cruz 2002)

Risk managers at banking companies face the problem to select and implement approaches to quantify operational risk. Single indicator approaches appear to be only suitable for small banking companies, for which the usage of more advanced approaches is too costly. Large banking companies usually have implemented stochastic methods, such as operational Value-at-Risk in connection with questioning techniques. This helps banking companies to determine the level of operational risk on base of a large number of historic data and expert opinions.

[1] Basel II approaches are based on indicator-approaches (such as Basic Indicator, Standardized Approach, Internal Measurement Approach or Scorecard Approach) as well as a stochastic method (Loss Distribution approach based on operational value-at-risk).

Further development of quantification methods for operational risk is still required. An integrated and consistent method is needed to quantify operational risk for the banking company as a whole and its business units. The creation of interfaces to other methods and risk types as well as a consistent aggregation of risk types is still a challenge.

Controlling Phase

Based on the identified and quantified operational risks, decisions on carrying, decreasing, avoidance as well as the transfer of the security risks are made within the controlling phase. There are internal and external controlling instruments for operational risks:

- Internal controlling instruments are focused on the sources and drivers of operational risk and are used to prevent loss events caused by operational risks.
- External controlling instruments aim at transferring operational risks out of the company. External parties carry potential losses caused by operational risks. Such instruments are insurance policies, outsourcing of process or systems and alternative risk transfer instruments, such as Operational Risk Linked Bonds.

Monitoring Phase

The monitoring phase encompasses all procedures and techniques, which are necessary for a continuous monitoring of operational risk. Thereby it is analyzed, if

- all the occurred events have been prior identified as possible events,
- the distribution of probabilities of occurrence of events and the distribution of severities of losses have been anticipated within the quantification phase,
- the selected controlling measures have lead to the desired results.

To summarize the state-of-the-art in each of the four presented phases of Operational Risk Management, Table 3 provides an overview on research questions in selected contributions:

Table 3. Overview on phases and research in selected contributions

Phase	Research questions	Method	Source

Identification	• Which methods can be used to identify operational risks?
	• How can identified operational risks be categorised?
	• How can sources and drivers of operational risks be analysed?
		Descriptive analysis	(Basel Committee on Banking Supervision 2001;
			Brink 2000; Cruz 2002;
			Eller et al. 2002; Jörg 2002;
			Faisst and Kovacs 2003;
			Lokarek-Junge and Hengmith 2003; Marshall 2001;
			Piaz 2001)

		Case study (N=20 banking companies)	(Hoffman 2002)

Quantification	• Which methods can be used to quantify operational risks?
	• How can operational risks be aggregated?
	• How can rare events with large severity be quantified?
		Descriptive analysis	(Brink 2000; Buhr 2000;
			Cruz 2002; Eller et al. 2002;
			Faisst and Kovacs 2003;
			Jörg 2002; Marshall 2001;
			Piaz 2001).

		Case study (N=20 banking companies)	(Hoffman 2002)
	• Which quantification method is suitable for which implementation area?	Descriptive analysis	(Faisst and Kovacs 2003)
	• Which amount of losses has been caused by operational risk (based on historical data)?	Empirical study (N=89 banking companies)	(Basel Committee on Banking Supervision 2004)
		Simulation model	(Beeck and Kaiser 2000)
	• How much does a business process contribute to the aggregated operational risk?	Simulation model	(Ebnöther et al. 2001)

Controlling	• Which instruments can be used to control the level of operational risk? • Which impact have these controlling instruments on the frequency and severity of events caused by operational risk?	Descriptive analysis	(Brink 2000; Cruz 2002; Eller et al. 2002; Jörg 2002; Lokarek-Junge and Hengmith 2003; Marshall 2001; Piaz 2001).
		Case study	(Spahr 2001)
		Case study (N=20 banking companies)	(Hoffman 2002)
Monitoring	• Which procedures and methods should be implemented to monitor operational risk? • Which requirements have to be considered to monitor operational risk in the most relevant business processes?	Descriptive analysis	(Basel Committee on Banking Supervision 2001; Basel Committee on Banking Supervision 2004; Brink 2000; Cruz 2002; Eller et al. 2002; Lokarek-Junge and Hengmith 2003; Marshall 2001; Piaz 2001).
		Case study (N=20 banking companies)	(Hoffman 2002)

This contribution focuses on the controlling phase and the steering of security risks by implementing security mechanism to prevent loss events (ex-ante) and using insurance policies to transfer parts of the losses in case of an event (ex-post). The contribution analyses, which combinations of ex-ante and ex-post controlling measures lead to an efficient solution.

A Controlling Model for Security Risks

The model aims to solve the described trade-off between the expected losses and the opportunity costs of the economical capital charge on the one hand and the investments in security mechanisms and insurance policies on the other. Thereby, the amount to be invested in security mechanisms and insurance policies will be optimized.

Assumptions

The time horizon accounts for a single period.

Assumption 1: Independence of a single information system

A single information system is regarded, neglecting possible dependencies to other information systems.

Assumption 2: Relevant cashflow parameters

The expected total negative cashflow μ of the information system is composed of the items expected losses due to security risks E(L), the opportunity costs of the economical capital charge OCC, the investments in security mechanisms I_{SM} and the investments in insurance policies I_{Ins}.

$$\mu = E(L) + OCC + I_{SM} + I_{Ins} \tag{1}$$

The cashflow items E(L), OCC, I_{SM} and I_{Ins} are estimated ex-ante.

Assumption 2a: Expected losses

The expected loss E(L) arises as a result of multiplying the expected frequency of attempted attacks λ by the expected loss given events LGE (with LGE>0). For simplicity, we assume constant LGE. We also assume, that investments in security mechanisms can reduce the expected frequency of attempted attacks λ ex-ante by the so called security level (SL=1-a). The security level represents the percentage of prevented attacks through the implementation of technical security mechanisms. In order to make allowance for the impacts of these mechanisms, the expected frequency of attempted attacks λ is multiplied by the factor a (whereby $0<a\leq1$) that represents the percentage of successful attacks. We further assume that investments in insurance policies can reduce the amount of losses LGE by the so called insurance level (IL=1-b). The insurance level represents the percentage of the transferred respective insured loss given events. In order to make allowance

for the impacts of insurance policies, the expected loss given events LGE are multiplied by the factor b (whereby 0<b≤1) that represents the percentage of not insured loss given events LGE. Thus, the expected losses E(L) are:

$$
\begin{aligned}
E(L) &= E[(a \cdot N) \cdot (b \cdot LGE)] \\
&= (a \cdot E(N)) \cdot (b \cdot LGE) \\
&= (a \cdot \lambda) \cdot (b \cdot LGE) \qquad (2)
\end{aligned}
$$

with:

$E(N)=\lambda$:= Expected frequency of attempted attacks N,

a:= Percentage of successful attacks,

LGE:= Expected loss given events,

b:= Percentage of not insured loss given events.

We assume, that the frequency of successful attacks Q is Poisson distributed. The Poisson distribution exhibits the characteristic that the variance corresponds to the expected value. The variance σ_Q^2 is determined by:

$$\sigma_Q^2 = E(Q) = a \cdot \lambda \qquad (3)$$

For constant LGE, the standard deviation of losses σ_L is given by:

$$\sigma_L = \sqrt{a \cdot \lambda} \cdot (b \cdot LGE) \qquad (4)$$

Assumption 2b: Opportunity costs of economical capital charge

Under the assumption 2a of Poisson distributed frequency of loss events and of constant LGE, the economical capital charge ECC can be determined as follows:

$$ECC = \gamma \cdot E(L) \qquad (5)$$

The economic capital charge ECC arises as a result of multiplying E(L) by the so-called gamma-factor γ[2]. With an opportunity interest rate r, the opportunity costs of the economical capital charge OCC are given by:

$$OCC = r \cdot ECC = r \cdot \gamma \cdot E(L) \qquad (6)$$

The opportunity costs of the economical capital charge OCC exhibit a deterministic character. The standard deviation σ_{OCC} is therefore given by:

$$\sigma_{OCC} = 0 \qquad (7)$$

[2] The gamma-factor translates the estimate of expected losses into an estimate for the unexpected losses to be covered by capital charge (Basel Committee on Banking Supervision 2001).

Assumption 2c: Investments in security mechanisms

According to assumption 2a, increasing investments in security mechanisms I_{SM} implicate decreasing expected losses E(L) et vice versa. We assume that the frequency of attempted attacks λ can be reduced ex-ante by implementing security mechanisms.

$$I_{SM} = \frac{\lambda \cdot LGE}{[a \cdot \lambda \cdot LGE]^{\beta}} - 1 \qquad (8)$$

with:

$I_{SM}=0$ for $a=\beta=1$;

$I_{SM}>0$ for $0<a<1$ and $0<\beta<1$.

According to assumption 2a and equation (8), there is an inversely proportional relationship between the investments in security mechanisms I_{SM} and the percentage of successful attacks a for a constant calibration factor β. This calibration factor determines the sensitivity of the relationship (whereby $0<\beta\leq 1$).

Similar to the opportunity costs of the economical capital charge, the investments in security mechanisms I_{SM} exhibit a deterministic character. The standard deviation σ_{SM} is therefore given by:

$$\sigma_{SM} = 0 \qquad (9)$$

Assumption 2d: Investments in insurance policies

According to assumption 2a, increasing investments in insurance policies I_{Ins} implicate decreasing E(L), et vice versa. If the security risks fulfil the criteria of insurability, banking companies are able to reduce the extent of damage ex-post by investments in insurance policies.

$$I_{Ins} = \left(\frac{\lambda \cdot LGE}{[b \cdot \lambda \cdot LGE]^{\delta}} - 1 \right) \qquad (10)$$

with:

$I_{Ins}=0$ for $b=\delta=1$;

$I_{Ins}>0$ for $0<b<1$ and $0<\delta<1$.

Analogous to the investments in security mechanisms we assume an inversely proportional relationship between the investments in insurance policies I_{Ins} and the percentage of not insured loss given events b for a constant calibration factor δ. This calibration factor determines the sensitivity of the relationship (whereby $0<\delta\leq 1$).

The investments in insurance policies I_{Ins} exhibit a deterministic character and the standard deviation is given by:

$$\sigma_{Ins} = 0 \qquad (11)$$

Assumption 3: Solution space with continuous σ and its transformation on μ(σ):

We assume that any number of $\sigma \in (0,\infty)$ exists and the corresponding cashflows can be mapped through the continuous function $\mu(\sigma)$.[3] Only one σ can be realized**,** combinations are not possible.

Determining the optimal security and insurance level

In order to determine the optimal security and insurance level (SL*, IL*) and the corresponding optimal amount to be invested in technical security mechanisms I^*_{SM} and insurance policies I^*_{Ins}, we assume a risk neutral decision-maker that aims at minimizing his expected total negative cashflow μ.

The expected total negative cashflow is obtained by the substitution of (2), (6), (8) and (10) in (1):

$$\begin{aligned}\mu &= (1+r\cdot\gamma)\cdot(a\cdot\lambda)\cdot(b\cdot \mathrm{LGE}) \\ &+\frac{\lambda\cdot \mathrm{LGE}}{(a\cdot\lambda\cdot \mathrm{LGE})^{\beta}}+\frac{\lambda\cdot \mathrm{LGE}}{(b\cdot\lambda\cdot \mathrm{LGE})^{\delta}}-2\end{aligned} \tag{12}$$

The derivation of equation (12) with respect to a is given by:

$$\frac{\partial\mu}{\partial a}=\lambda\cdot(1+r\cdot\gamma)\cdot(b\cdot \mathrm{LGE})-\beta\cdot\frac{\lambda\cdot \mathrm{LGE}}{(\lambda\cdot \mathrm{LGE})^{\beta}\cdot a^{\beta+1}} \tag{13}$$

$$\frac{\partial^2\mu}{\partial^2 a}=\beta\cdot(\beta+1)\cdot\frac{\lambda\cdot \mathrm{LGE}}{(\lambda\cdot \mathrm{LGE})^{\beta}\cdot a^{\beta+2}}>0 \tag{14}$$

Equation (13) fulfils the necessary as well as (13) and (14) the sufficient conditions of a minimum of the expected total negative cashflow. Transformation of (13) leads to:

$$a=\frac{\left(\frac{\beta\cdot\lambda\cdot \mathrm{LGE}}{b\cdot(1+r\cdot\gamma)}\right)^{\frac{1}{\beta+1}}}{\lambda\cdot \mathrm{LGE}} \tag{15}$$

The derivation of the variable b is obtained analogous and is given by:

$$b=\frac{\left(\frac{\delta\cdot\lambda\cdot \mathrm{LGE}}{a\cdot(1+r\cdot\gamma)}\right)^{\frac{1}{\delta+1}}}{\lambda\cdot \mathrm{LGE}} \tag{16}$$

Substitution of (16) in (15) and (15) in (16) leads to

[3] Thus, it is assumed that any number of σ can be obtained. In reality only a finite number of discrete values of σ exist. Another simplification is the assumption that for any number of σ a continuous function μ(σ) exists.

$$a^* = (\lambda \cdot \mathrm{LGE})^{\frac{\delta-\beta(\delta+1)}{\beta\cdot(\delta+1)+\delta}} \cdot \left(\frac{\beta^{(1+\delta)}}{\delta\cdot(r\cdot\gamma+1)^{\delta}}\right)^{\frac{1}{\beta\cdot(\delta+1)+\delta}} \tag{17}$$

$$b^* = (\lambda \cdot \mathrm{LGE})^{\frac{\beta-\delta\cdot(\beta+1)}{\beta\cdot(\delta+1)+\delta}} \cdot \left(\frac{\delta^{(1+\beta)}}{\beta\cdot(r\cdot\gamma+1)^{\beta}}\right)^{\frac{1}{\beta\cdot(\delta+1)+\delta}} \tag{18}$$

The optimal security level SL^* and insurance level IL^* are (see assumption 2a)

$$SL^* = 1 - a^* \tag{19}$$

$$IL^* = 1 - b^* \tag{20}$$

and therefore obtained by substitution of (17) in (19) and (18) in (20):

$$\mathrm{SL}^* = 1 - \left[(\lambda \cdot \mathrm{LGE})^{\frac{\delta-\beta\cdot(\delta+1)}{\beta\cdot(\delta+1)+\delta}} \cdot \left(\frac{\beta^{(1+\delta)}}{\delta\cdot(r\cdot\gamma+1)^{\delta}}\right)^{\frac{1}{\beta\cdot(\delta+1)+\delta}} \right] \tag{21}$$

$$\mathrm{IL}^* = 1 - \left[(\lambda \cdot \mathrm{LGE})^{\frac{\beta-\delta\cdot(\beta+1)}{\beta\cdot(\delta+1)+\delta}} \cdot \left(\frac{\delta^{(1+\beta)}}{\beta\cdot(r\cdot\gamma+1)^{\beta}}\right)^{\frac{1}{\beta\cdot(\delta+1)+\delta}} \right] \tag{22}$$

The minimum of the expected total negative cashflow $\mu^*(a^*,b^*)$ is obtained by the substitution of the equations (17) and (18) in equation (12). In doing so, it is further possible to determine the optimal amount to be invested in security mechanisms I^*_{SM} and insurance policies I^*_{Ins}:

$$I^*_{SM} = \frac{\lambda \cdot \mathrm{LGE}}{\left[(\lambda \cdot \mathrm{LGE})^{\left(\frac{2\cdot\delta}{(1+\delta)\cdot\beta+\delta}\right)} \cdot \left(\frac{\beta^{(1+\delta)}}{\delta\cdot(1+r\cdot\gamma)^{\delta}}\right)^{\left(\frac{1}{(1+\delta)\cdot\beta+\delta}\right)} \right]^{\beta}} - 1 \tag{23}$$

$$I^*_{Ins} = \frac{\lambda \cdot \mathrm{LGE}}{\left[(\lambda \cdot \mathrm{LGE})^{\left(\frac{2\cdot\beta}{(1+\delta)\cdot\beta+\delta}\right)} \cdot \left(\frac{\delta^{(1+\beta)}}{\beta\cdot(1+r\cdot\gamma)^{\delta}}\right)^{\left(\frac{1}{(1+\delta)\cdot\beta+\delta}\right)} \right]^{\delta}} - 1 \tag{24}$$

The mapped area in Fig. 3 illustrates all possible μ(a,b)-combinations and the corresponding security and insurance level (SL,IL) for given values of β and σ. However, there is only one minimum in μ*(a*,b*) and therefore only one efficient (SL*,IL*)-solution.

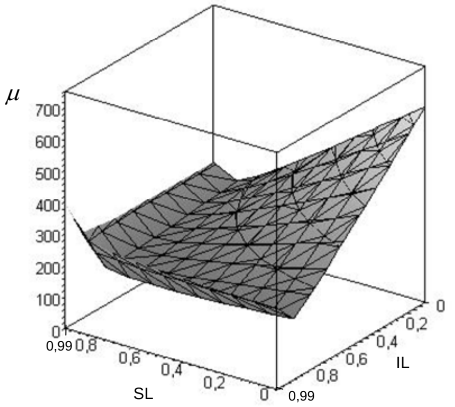


Fig. 3. Minimum of the expected total negative cashflow[4]

Example 1: Consider the following instance for the model: $\beta = 0{,}2$; $\delta = 0{,}6$; $r = 0{,}1$; $LGE = 1.000$; $\lambda = 0{,}3$; $\gamma = 7{,}3$. The optimal security and insurance level are given by $SL^* = 0{,}58$ (with $a^* = 0{,}42$) and $IL^* = 0{,}9$ (with $b^* = 0{,}1$). Therefore a banking company would invest $I^*_{SM} = 112{,}99$ in technical security mechanisms and $I^*_{Ins} = 36{,}99$ in insurance policies. The expected loss E(L) equals the value $E(L) = 13{,}18$ and the opportunity costs of the economical capital charge $OCC = 9{,}62$. Therefore the minimum of the expected total negative cashflow is given by $\mu^* = 172{,}78$.

Result 1: **For any given values of (β, δ) only one minimum of the expected total negative cashflow μ*(a*,b*), respective (SL*, IL*)-solution exists.**

[4] According to assumption 2a, the domains of a, b and SL, IL respectively are given by $a, b \in]0; 1]$ and $SL, IL \in [0; 1[$. The closer SL, IL approaches to 1, the greater the expected total negative cashflow μ . Therefore, μ is not limited and can rise infinitely. For illustration reasons, the plotted graph shows all the SL, IL -combinations within the domain [0; 0,99].

Constraints and their impacts

In practice, constraints like limited economical capital charge and limited budget affect the controlling of security risks. We will further analyze the impacts of such constraints.

At first, we transform the expected total negative cashflow in an equation dependent on the standard deviation. The standard deviation of the expected total negative cashflow σ_{ETNC} arises by considering (3), (7), (9) and (11):

$$\sigma_{ETNC} = \sigma_L = \sqrt{a \cdot \lambda} \cdot (b \cdot LGE) \tag{23}$$

$$a \cdot \lambda = \frac{\sigma_{ETNC}^2}{(b \cdot LGE)^2} \tag{24}$$

In the following, σ_{ETNC} is denoted as σ. We obtain E(L), OCC, and I_{SM} in dependence of σ by the substitution of (24) in (2), (6), (8) and (10):

$$E(L) = \frac{\sigma^2}{b \cdot LGE} \tag{25}$$

$$OCC = r \cdot \gamma \cdot \frac{\sigma^2}{b \cdot LGE} \tag{26}$$

$$I_{SM} = \frac{\sigma^2}{a \cdot b^2 \cdot LGE \cdot \left(\frac{\sigma^2}{b^2 \cdot LGE} \right)^{\beta}} - 1 \tag{27}$$

$$I_{Ins} = \frac{\sigma^2}{a \cdot b^2 \cdot LGE \cdot \left(\frac{\sigma^2}{a \cdot b \cdot LGE} \right)^{\delta}} - 1 \tag{28}$$

The expected total negative cashflow $\mu(\sigma)$ is obtained based on (25), (26), (27) and (28):

$$\mu = \frac{\sigma^2}{b \cdot LGE} \cdot \left(1 + r \cdot \gamma + \frac{1}{a \cdot b} \cdot \left(\left(\frac{b^2 \cdot LGE}{\sigma^2} \right)^{\beta} + \left(\frac{a \cdot b \cdot LGE}{\sigma^2} \right)^{\delta} \right) \right) - 2 \tag{29}$$

Equation (29) describes $\mu(\sigma)$ as a continuous function in dependence of σ. $\mu(\sigma)$ thereby maps the domain $\sigma \in (0;\infty)$ well defined on $\mu(\sigma) \in (\mu^*;\infty)$. Fig. 4 illustrates the trade-off between the expected losses E(L) and the opportunity costs of the economical capital charge OCC on the one hand and the investments in security mechanisms I_{SM} and insurance policies I_{Ins} on the other. The expected total negative cashflow $\mu(\sigma)$ thereby possesses only one minimum in $\mu^*(\sigma^*)$.

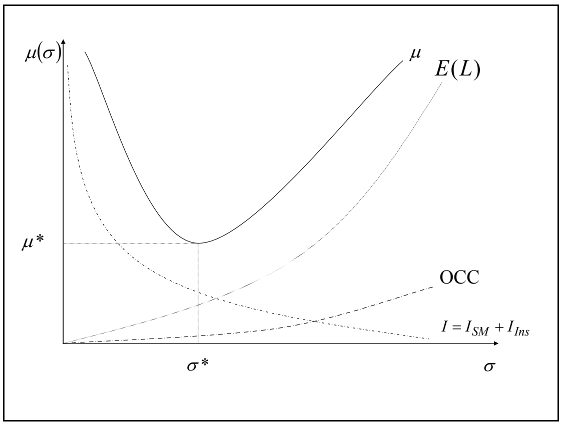


Fig. 4. Trade off between E(L) and OCC on the one hand and I_{SM} and I_{Ins} on the other

Example 2: Analogous to example 1, we consider the following instance for the model: β=0,2; δ=0,6; r=0,1; LGE=1.000; λ=0,3; γ=7,3; SL*=0,58 (with a*=0,42); IL*=0,9 (with b*=0,1) and μ*=172,78. Substituting these values in (29) leads to an optimal risk level amounting to σ*=36,17.

As mentioned above, the minimum of the expected total negative cashflow μ*(a*,b*), respectively (SL*,IL*))-solution, is derived by equation (12) in connection with (19) and (20). The appropriate optimal risk level σ* can be determined by equation (29) in conjunction with μ*.

Constraint 1: Risk limits of the economical capital charge

Composing limits of the economical capital charge determines the amount of risks a banking company is prepared to carry. In addition, we assume that a banking company defines a limit of the economical capital charge LECC for a single information system. In doing, so the amount of feasible solutions is restricted. In order to illustrate the impacts on the expected total negative cashflow, we consider two different limits of the economical capital $LECC_i$ (i=1,2).

The two limits $LECC_{1,2}$ are represented in Fig. 5. $LECC_1$ cuts the expected total negative cashflow in (μ_1,σ_1). In this case, the banking company is further able to realize the global minimum of the expected total negative cashflow in (μ*,σ*). Therefore, the limit of the economical capital charge $LECC_1$ does not tap the full potential ($\sigma^*<\sigma_1$).

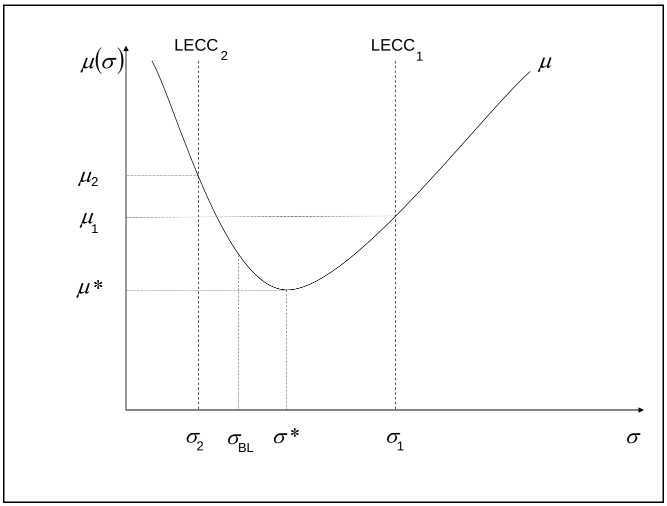


Fig. 5. Risk limits of economical capital charge

However, in the second case the limit LECC$_2$ cuts the expected total negative cashflow in the suboptimal solution (μ_2,σ_2). The expected total negative cashflow μ_2 is greater than μ*, the corresponding risk σ_2 is accordingly smaller (σ_2<σ*).

Result 2: **In case the LECC exceeds the optimal solution (μ*,σ*), a banking company can further realize the minimal expected total negative cashflow μ*. However, if the LECC is smaller than σ* a banking company can only realize suboptimal solutions.**

Analogous to the limits of the economical capital charge, budget limits restrict the amount of feasible solutions. Their impacts are analyzed in the following.

Constraint 2: Budget limits

Budget limits BL serve as a limitation of the payments in business areas or in our case in information systems. Budgeting generally considers the expected losses E(L) ex-ante. Anyhow, L is a random variable that can exceed ex-post the defined budget limit. The amount exceeded can be covered through equity capital. Fig. 6 illustrates the impact of the budget limit BL exemplarily. A budget limit BL cuts the expected total negative cashflow in the suboptimal solution (μ_{BL},σ_{BL}). In this case, a banking company can further realize the optimal solution (μ*,σ*). Assumed that the budget limit BL is smaller than the optimal solution (μ*,σ*), the information system cannot be carried on.

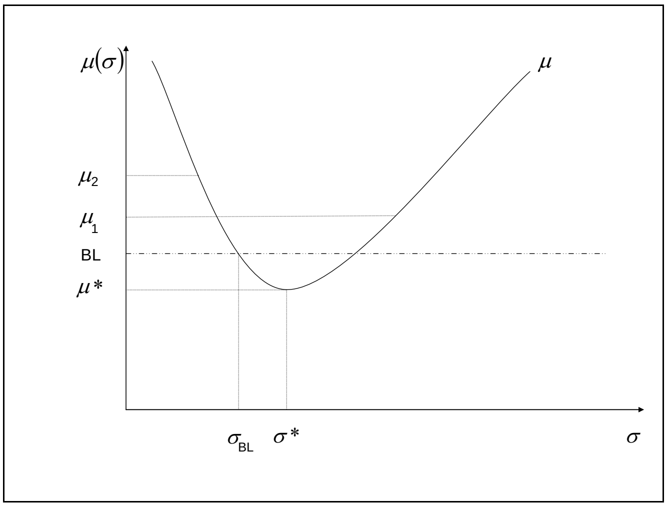


Fig. 6. Budget limits

Result 3: **If the budget limit BL exceeds the minimal expected total negative cashflow BL≥µ*, a risk neutral decision maker will further choose the optimal solution (µ*,σ*).**

Conclusion

The developed decision model is able to map the existing trade-off between the expected losses and the opportunity costs of the economical capital charge on the one hand as well as the investments in security mechanisms and insurance policies on the other hand in a common framework. Thereby, the model optimizes the investments in ex-ante and ex-post controlling mechanisms. Only one (a*,b*)-respective (SL*,IL*)-combination exists that minimizes the expected total negative cashflow. Furthermore, the model points out that the constraints - limits of the economical capital charge and budget limits - can, under certain conditions, lead to suboptimal solutions. Normally a banking company determines its limits centrally via an individual information system. Not fully taped limits of economical capital charge and budget limits cannot be exchanged. Thus, this can lead to inefficiencies from a holistic point of view. The exchange of not fully taped potentials can implicate a greater utility.

However, further research questions arise from the defined assumptions:

- In the model an isolated information system is regarded, by which it is assumed that it is independent of all other systems. Correlations to other information systems are not considered. Taking correlations into account can lead to different results.

- We further assume that investments in security mechanisms and insurance policies can be mapped within the domain of $\sigma \in (0;\infty)$. This can be traced back to the property of continuity of the function $\mu(\sigma)$. It is assumed that in reality only discrete action alternatives exist.
- For simplicity, we assumed constant loss given events. However, if the standard deviation of the expected loss given events is taken into account, the expected total negative cashflow will be affected. A further research topic includes modeling random variables for the loss given events.

References

Basel Committee on Banking Supervision (2001) Working Paper on the Regulatory Treatment of Operational Risk. Retrieved December 12, 2005, from www.bis.org/publ/bcbs_wp8.pdf

Basel Committee on Banking Supervision (2004) Internal Convergence of Capital Measurement and Capital Standards. Retrieved December 12, 2005, from http://www.bis.org/publ/bcbs107.pdf

Beeck H, Kaiser, T (2000) Quantifizierung von Operational Risk. In: Johanning, L., Rudolph, B. (eds.) Handbuch Risikomanagement. UHLENBRUCH Verlag, Bad Soden/Ts, pp 633-654

Brink J. van den (2000) Operational Risk: Wie Banken das Betriebsrisiko beherrschen. Dissertation, St. Gallen, Switzerland

BSI (2004) IT-Grundschutzhandbuch. Retrieved March 12, 2004, from http://www.bsi.de/gshb/deutsch/download/GSHB2004.pdf

Buhr, R (2000) Messung von Betriebsrisiken – ein methodischer Ansatz. Die Bank 40: 202-206

Cruz A (2002) Modeling, Measuring and Hedging Operational Risk. John Wiley & Sons, Chichester

CSI/FBI (2005) Computer Crime and Security Survey 2005. Retrieved April 9, 2005, from http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf

Ebnöter S, Vanini P, McNeil A, Antolinez-Fehr, P (2001) Modelling Operational Risk. Working Paper, ETH Zürich

Eller R, Gruber W, Reif M (2002) Handbuch Operationelle Risiken – Aufsichtsrechtliche Anforderungen, Quantifizierung und Management, Praxisbeispiele. Schäffer-Poeschel Verlag, Stuttgart

Faisst U (2004) Ein Modell zur Steuerung operationeller Risiken in IT-unterstützten Bankprozessen. Banking and Information Technology (BIT) - Sonderheft zur Multikonferenz Wirtschaftsinformatik 2004 in Essen 1: 35-50

Faisst U, Kovacs M (2003) Quantifizierung operationeller Risiken - ein Methodenvergleich. Die Bank 43: 342-349

Gemela J (2001) Financial analysis using Bayesian networks. Applied Stochastic Models in Business and Industry 17: 57-67

Hoffman D G (2002) Managing Operational Risk – 20 Firmwide Best Practice Strategies. John Wiley & Sons, Chichester

Jörg M (2002) Operational Risk – Herausforderung bei der Implementierung von Basel II. Diskussionsbeiträge zur Bankbetriebslehre, Hochschule für Bankwirtschaft, Frankfurt, Germany

Locarek-Junge H, Hengmith L (2003) Management des operationalen Risikos der Informationswirtschaft in Banken. In: Geyer-Schulz A, Taudes A (eds.) Informationswirtschaft: Ein Sektor mit Zukunft – Symposium. Köllen Druck + Verlag, Bonn

Marshall C L (2001) Measuring and Managing Operational Risk in Financial Institutions. John Wiley & Sons, Chichester

Müller G, Eymann T, Kreutzer M (2003) Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft. Oldenbourg, München

Müller G, Rannenberg K (1999) Multilateral Security in Communications. Vol. 3: Technology, Infrastructure, Economy. Addison-Wesley-Longman, New York

Piaz J M (2001) Operational Risk Management bei Banken. Versus-Verlag, Zürich

Rannenberg K (1998) Zertifizierung Mehrseitiger Sicherheit: Kriterien und organisatorische Rahmenbedingungen. Vieweg, Braunschweig, Wiesbaden

Sackmann S, Strüker J (2005) 10 Jahre E-Commerce - Eine stille Revolution in deutschen Unternehmen. Konradin Verlag, Leinfelden

Spahr R (2001) Steuerung operationaler Risiken im Electronic und Investment Banking. Die Bank 41: 660-663