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

Universität Augsburg
University

Discussion Paper WI-152

An Optimization Model for the Management of Security Risks in Banking Companies

by

Ulrich Faisst, Oliver Prokein[1]

April 2005

presented at: Müller, G., Lin, K.-J., Proceedings of the 7th IEEE International Conference on E-Commmerce Technology (CEC) 2005, München, July 2005, IEEE Computer Society Press, Los Alamitos, CA, 2005, p.266-273

[1] Institut für Informatik und Gesellschaft, Universität Freiburg

An Optimization Model for the Management of Security Risks in Banking Companies

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

Oliver Prokein
Institute of Computer Science and Social Studies,
Department of Telematics
University of Freiburg
email: oliver.prokein@iig.uni-freiburg.de

Abstract

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 accept Expected Losses 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. This paper contributes to the development of an optimization model that aims 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 and is supposed to help practitioners in controlling Security Risks.

1. Introduction

Due to the increasing virtualization of business processes and the cumulative adoption of ICT involved, Security Risks have lately gained in significance. 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 [12].

However, the rising deployment of ICT implicates increasing Security Risks. Increasing Investments in Technical Security Mechanisms and Insurance Policies generally lead to lower Expected Losses and Opportunity Costs of the Regulatory Capital Charge, et vice versa [4]. Thus, a trade-off exists between the Expected Losses and the Opportunity Costs of the Regulatory 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 company. In case, where an explicit responsibility exists, the decision-maker will 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 will tend to minimize costs and therefore neglects further investments, although such investments are profitable in a holistic view.

This paper 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 Regulatory 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 lay the basic principles for the model we will first portray the risk management process.

2. The Risk Management Process

The activities of risk management can be illustrated according to the risk management process. The process contains the four phases of identification, quantification, controlling and monitoring [10]. The risk management process is illustrative and may not be interpreted as a unique operational sequence. In practice, it is necessary to improve the process continuously and challenge the results critically.

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 [8]. 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 [9]. Therefore, the analysis of security requires not only the observation of external attackers but also the inclusion of all parties involved as potential attackers. The concept of multilateral security [9] 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 [11]:

- *Loss of Confidentiality*, i.e. the risk of unauthorized gain of information.
- *Loss of Integrity*, i.e. the risk of unauthorized modification or erasure of information and data.
- *Loss of Accountability*, i.e. the risk of illegal irresponsibility.
- *Loss of Availability*, i.e. the risk of unauthorized impairment of the functionality.

Table 1: Economic impacts of attacks

Protection Goals	Selected Attacks	Potential Economic Impacts
Confiden-tiality	Hacker-Attacks, Industry-Spying, 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.
Account-ability	IP-Spoofing, Social Hacking, Inadequate Access Control etc.	Loss of Image, Business Interruption, Liability Claims of Third etc.
Availability	DDOS, Virus, Hard Failure etc.	Loss of Recovery, Loss of Market Share etc.

Table 1 illustrates selected attacks and their potential economic impacts. The probability of loss occurrence arises from the observed attacks, the amount of losses from the economic impacts.

Quantification Phase

The identified Security Risks are measured by the use of different methods within the quantification phase [3]. So far, no quantification model has been developed for the measurement of the Security Risks, defined above. These Security Risks are however a subset of Operational Risks. The Basel Committee on Banking Supervision defines Operational Risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events [2].[1] For the measurement of this Operational Risk the committee suggests five different quantification methods in order to determine the Regulatory Capital Charge. The models reach from simple, factor-based approaches to complex stochastic loss distribution models based on the Value-at-Risk [1], [2]. Beyond that, further methods exist for the quantification of Operational Risks, as for instance questioning techniques or causal methods, like Bayesian Belief Networks [8].

Controlling Phase

Based on the identified and quantified Security Risks, decisions on carrying, decreasing, avoidance as well as the transfer of the Security Risks are made within the controlling phase.

Technical Security Mechanisms can be used to control ex-ante Security Risks. Table 2 illustrates selected Security Mechanisms. We assume that Security Mechanisms are appropriate for reducing the Expected Loss Frequency of successful attacks ex-ante.

Table 2: Protection goals and Security Mechanisms

Protection Goals	Selected Security Mechanisms
Confidentiality	Symmetric and Asymmetric Cryptography, Firewalls, VPN, Stenography, Broadcast etc.
Integrity	Digital Signatures, Message Authentication Codes, Virus Scanner etc.
Accountability	Digital Signatures, Public-Key-Infrastructures, Watermaking etc.
Availability	Patches, Backup-Systems, IDS, Physical Protection, etc.

Moreover, banking companies are able to transfer the amount of losses *ex-post* by Insurance Policies. However, due to the characteristics, not every security risk is insurable. Various catalogues of criteria have been developed in the past in order to examine insurability. The five criteria of KARTEN are referred to below [7]:

- The criterion of *fortuitousness* demands that the event causing the case has to be uncertain and unaffected.

[1] This definition includes legal risk, but excludes strategic and reputational risk.

- *Unambiguousness* assumes that the occurrence and the amount of losses are verifiable in an objective way.
- *Estimability* targets the problem of insufficient knowledge. An insurance company must be able to estimate the probability of occurrence and the average amount of losses.
- *Independence* refers to positively related risks that should be excluded so as to ensure a process of fortuity of the insured loss given events of the business in force.
- The last criteria, *size* refers to the maximum damage that can result from a single risk. Because it is difficult to quantify the damages exactly, insurance companies only agree to cover a certain percentage of the amount of losses.

With regard to these criteria, *table 3* illustrates that only threats of the protection goals integrity and availability are insurable [6].

Table 3: Insurability of Security Risks

Protection Goals	Insurability	Problems
Confidentiality	Not Applicable	Definite Causal Connection, provability, quantification
Integrity	Yes	Low Limits of Coverage, Expensive Technical Security Precautions
Accountability	Not Applicable	Definite Causal Connection, Provability
Availability	Yes	Low Limits of Coverage, Expensive Technical Precautions

Monitoring Phase

The *monitoring phase* encompasses all procedures and techniques, which are necessary for a continuous monitoring of the Security Risks. 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.

This paper focuses on the controlling phase. In the following it will be investigated, which combinations of ex-ante and ex-post controlling measures lead to an efficient solution.

3. A Controlling Model for Security Risks

The model aims to solve the trade-off between the Expected Losses and the Opportunity Costs of the Regulatory 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.

3.1 Assumptions *(in italics)*

The time horizon accounts for a single period.

Assumption 1: Independence of a Single Information System

In the following, an open single information system is regarded. It is assumed that no dependencies exist 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 Regulatory Capital Charge* RCC*, the Investments in Security Mechanisms* I_{SM} *and the Investments in Insurance Policies* I_{Ins}*.*

$$\mu = E(L) + RCC + I_{SM} + I_{Ins} \quad (1)$$

The stochastic cashflow item L as well as the deterministic cashflow items RCC, I_{SM} and I_{Ins} are estimated ex-ante.

Assumption 2a: Expected Losses due to Security Risks

As mentioned in Chapter 2, the Basel Committee on Banking Supervision proposes five different approaches to quantify Operational Risks, such as Security Risks. The proposed Internal Measurement Approach [2] is modified to quantify the Expected Losses $E(L)$*.*

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

whereas: $E(N) = \lambda :=$ *Expected Frequency of Occurrence*[2]*,*
$a :=$ *Percentage of Successful Attacks,*
$LGE :=$ *Expected Loss Given Events,*
$b :=$ *Percentage of not Insured Loss Given Events.*

According to the Internal Measurement Approach $E(L)$ arises as a result of multiplying the expected frequency of occurrence λ by the Expected Loss Given Events LGE (with $LGE > 0$). For simplicity, we assume constant LGE. We assume, that Investments in Security Mechanisms can reduce the Expected Frequency of Occurrence 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 Occurrence is multiplied by the factor a (whereby $0 < a \leq 1$) 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 are multiplied by the factor b (whereby $0 < b \leq 1$) that represents the percentage of not insured loss given events.

The Internal Measurement Approach assumes a binomial-distribution for λ. However, the binomial distribution approaches the poisson distribution for large numbers of observed attacks with a small probability of occurrence. The poisson distribution exhibits the characteristic that the variance corresponds to the expectancy value.

$$\sigma^2 = a \cdot \lambda \quad (3).$$

For constant LGE, the standard deviation of Security Risks is given by:

$$\sigma_{SR} = \sqrt{a \cdot \lambda}\,(b \cdot LGE) \quad (4).$$

2 In the following, we refer to E(N) as λ. The Basel Committee on Banking Supervision defines the Expected Frequency of Occurrence $E(N) = \lambda$ as a the product of an Exposure Indicator (EI) with the Probability of Events (PE) per exposure. Therefore N is a random variable of the Loss Frequency.

Assumption 2b: Opportunity Costs of Regulatory Capital Allocation

According to the Internal Measurement Approach [1], the Regulatory Capital Charge K is given by:

$$K = \gamma \cdot E(L) \quad (5)$$

The Capital Charge K arises as a result of multiplying $E(L)$ by the so-called gamma-factor γ[3]*. With an interest rate of r, the Opportunity Costs of the Regulatory Capital Charge RCC are given by:*

$$RCC = r \cdot K = r \cdot \gamma \cdot E(L) \quad (6).$$

The Opportunity Costs RCC exhibit a deterministic character. The standard deviation σ_{RCC} is therefore given by:

$$\sigma_{RCC} = 0 \quad (7).$$

Assumption 2c: Investments in Security Mechanisms

We assume that the Probability of Loss Occurring λ can be reduced ex-ante by implementing Security Mechanisms.

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

whereby $I_{SM} = 0$ *for* $a = \beta = 1$
and $I_{SM} > 0$ *for* $0 < a < 1 \ \wedge \ 0 < \beta < 1$.

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 $0 < \beta \leq 1$). According to assumption 2a, increasing Investments in Security Mechanisms I_{SM} implicate decreasing Expected Losses $E(L)$ et vice versa.

Similar to the Opportunity Costs, the Investments in Security Mechanisms I_{SM} exhibit a deterministic character. The standard deviation is therefore given by:

$$\sigma_{SM} = 0 \quad (9).$$

3 The gamma-factor translates the estimate of Expected Losses into a Capital Charge [1].

Assumption 2d: Investments in Insurance Policies

If the Security Risks fulfill the criteria of insurability, banking companies are able to reduce the extent of damage ex-post by Investments in Insurance Policies.

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

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

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

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 $0 < \delta \leq 1$). According to assumption 2a, increasing Investments in Insurance Policies I_{Ins} implicate decreasing $E(L)$, et vice versa.

The Investments in Insurance Policies I^{SM} exhibit a deterministic character and the standard deviation is given by:

$$\sigma_{Ins} = 0 \quad (11).$$

Assumption 3: Solution Space with continuous σ and its transformation on $\mu(\sigma)$:

We assume that any number of $\sigma \in (0, \infty)$ exists and the corresponding cashflows can be mapped through the continuous function $\mu(\sigma)$.[4] Only one σ can be realized**,** combinations are not possible.

3.2 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):

$$\mu = (1 + r \cdot \gamma)(a \cdot \lambda)(b \cdot LGE) + \frac{\lambda \cdot LGE}{\left(a \cdot \lambda \cdot LGE \right)^{\beta}} + \frac{\lambda \cdot LGE}{\left(b \cdot \lambda \cdot LGE \right)^{\delta}} - 2 \quad (12).$$

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

$$\frac{\partial \mu}{\partial a} = \lambda(1 + r\gamma)(bLGE) - \beta \frac{\lambda \cdot LGE}{(\lambda \cdot LGE)^{\beta} \cdot a^{\beta+1}} \quad (13),$$

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

Equation (13) fulfills the necessary and (14) the sufficient condition of a minimum of the Expected Total Negative Cashflow. Transformation of (13) leads to:

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

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

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

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

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

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

The optimal Security Level SL^* and Insurance Level IL^* are (see assumption 2a)

$$SL^* = 1 - a^* \quad (19),$$

$$IL^* = 1 - b^* \quad (20),$$

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

4 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 $\mu(\sigma)$ exists.

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

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

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}.

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

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

The mapped area in *figure 1* illustrates all possible $\mu(a,b)$-combinations and the corresponding security and Insurance Level (SL, IL) for given values of β and δ. However, there is only one minimum in $\mu^*(a^*, b^*)$ and therefore only one efficient (SL^*, IL^*)-solution.

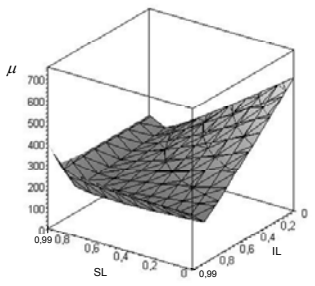

Figure 1: Minimum of the Expected Total Negative Cashflow.[5]

Example 1: Consider the following instance for the model: $\beta = 0{,}2$, $\delta = 0{,}6$, $r = 0{,}1$, $LGE = 1.000$, $\lambda = 0{,}3$ and $\gamma = 7{,}3$.
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 equals the value $E(L) = 13{,}18$ and the Opportunity Costs of the Regulatory Capital Charge $RCC = 9{,}62$. 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 $\mu^*(a^*, b^*)$, respective (SL^*, IL^*)-solution exists.**

3.3 Constraints and their Impacts

In practice, constraints like limits for Regulatory Capital Charge and Budget Limits affect the controlling of Security Risks. We will further analyze the impacts of constraints on the minimal Expected Total Negative Cashflow μ^*.

In order to analyze the impacts, we will first 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):

$$\sigma_{ETNC} = \sigma_{SR} = \sqrt{a \cdot \lambda}\,(b \cdot LGE) \quad (23).$$

$$\Rightarrow \; a \cdot \lambda = \frac{\sigma^2_{ETNC}}{(b \cdot LGE)^2} \quad (24)$$

In the following, σ_{ETNC} is denoted as σ.

We obtain EL, RCC, and I^{SM} in dependence of σ by the substitution of (24) in (2), (6) and (8):

$$EL = \frac{\sigma^2}{b \cdot LGE} \quad (25)$$

$$RCC = r \cdot \gamma \frac{\sigma^2}{b \cdot LGE} \quad (26)$$

5 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].

$$I^{SM} = \left(\frac{b}{\sigma}\right)^{2\beta} \cdot \lambda \cdot LGE^{1+\beta} - 1 \quad (27)$$

The Expected Total Negative Cashflow $\mu(\sigma)$ is obtained based on (25), (26), (27) and (10):

$$\mu = (1 + r \cdot \gamma) \cdot \frac{\sigma^2}{b \cdot LGE} + \left(\frac{b}{\sigma}\right)^{2\beta} \cdot \lambda \cdot LGE^{\beta+1} + \frac{b \cdot LGE}{(b \cdot \lambda \cdot LGE)^{\delta}} - 2 \quad (28)$$

Equation (26) describes $\mu(\sigma)$ as a continuous function in dependence of σ. $\mu(\sigma)$ thereby maps the domain $\sigma \in (0, \infty)$ well defined on $\mu(\sigma) \in (\mu^*, \infty)$. *Figure 2* illustrates the trade-off between the Expected Losses $E(L)$ and the Opportunity Costs of the Regulatory Capital Charge RCC 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 $\mu^*(\sigma^*)$.

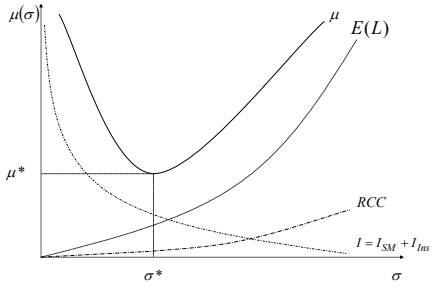

Figure 2: Trade-off between $E(L)$ and RCC on the one hand and I_{SM} and I_{Ins} on the other.

Example 2: Analogous to example 1, we consider the following instance for the model: $\beta = 0{,}2$, $\delta = 0{,}6$, $r = 0{,}1$, $LGE = 1.000$, $\lambda = 0{,}3$, $\gamma = 7{,}3$, $SL^* = 0{,}58$ (with $a^* = 0{,}42$), $IL^* = 0{,}9$ (with $b^* = 0{,}1$). and $\mu^* = 172{,}78$. Substituting these values in (26) leads to an optimal risk level amounting to $\sigma^* = 36{,}17$.

As mentioned above, the minimum of the Expected Total Negative Cashflow $\mu^*(a^*, b^*)$, 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 (26) in conjunction with μ^*.

Constraint 1: Limits of the Regulatory Capital Charge

Composing Limits of the Regulatory Capital Charge determines the amount of risks a banking company is prepared to carry. We now assume that a banking company defines a Limit of the Regulatory Capital Charge $LRCC$ 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 Regulatory Capital Capital $LRCC_i$ (i = 1,2).

The two limits $LRCC_{1,2}$ are represented in *figure 2*. $LRCC_1$ 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 Regulatory Capital Charge $LRCC_1$ does not tap the full potential $(\sigma^* < \sigma_1)$.

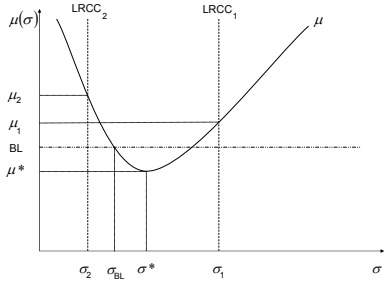

Figure 3: Consideration of Budget Limits and limits of Regulatory Capital Charge.

However, in the second case the limit $LRCC_2$ 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 is accordingly smaller $(\sigma_2 < \sigma^*)$.

Result 2: **In case the $LRCC$ exceeds the optimal solution (μ^*, σ^*), a banking company can further realize the minimal Expected Total Negative Cashflow (μ^*, σ^*). However, if the $LRCC$ is smaller than (μ^*, σ^*) a banking company can only realize suboptimal solutions.**

In addition to the Limit of the Regulatory Capital Charge, Budget Limits are further constraints. Their impacts are analyzed in the following.

Constraint 2: Budget Limits

Budget Limits serve as a limitation of the payments in business areas or in our case in information systems. Analogous to the Limits of the Regulatory Capital Charge, Budget Limits restrict the amount of feasible solutions. Budgeting generally considers the Expected Losses $E(L)$ ex-ante. Anyhow, SR is a random variable that can exceed ex-post the defined Budget Limit. The amount exceeded can be covered through equity capital. *Figure* 3 illustrates the impact of the Budget Limit BL exemplarily. 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.

Result 3: **If the Budget Limit BL exceeds the minimal Expected Total Negative Cashflow $BL \geq \mu^*$, a risk neutral decision maker will further choose the optimal solution (μ^*, σ^*).**

4. Conclusion

The developed decision model is able to map the existing trade-off between the Expected Losses and the Opportunity Costs of the Regulatory 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 Regulatory 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 Regulatory 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.

5. References

[1] Basel Committee on Banking Supervision: Regulatory Treatment of Operational Risk. Working Paper No. 8, 2001.

[2] Basel Committee on Banking Supervision: The New Basel Capital Accord, 2003.

[3] Cruz, A.: Modeling, Measuring and Hedging Operational Risk. John Wiley & Sons, 2002.

[4] Faisst, U.: Ein Modell zur Steuerung operationeller Risiken in IT-unterstützten Bankprozessen, Multikonferenz Wirtschaftsinformatik, Essen, 2004.

[5] Faisst, U., and Kovacs, M.: Quantifizierung operationeller Risiken – ein Methodenvergleich. Die Bank, Nr. 5, 2003, p. 342-349.

[6] Grzebiela, T.: Insurability of Electronic Commerce Risks. Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.

[7] Karten, W.: Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsnehmers – betriebswirtschaftliche Aspekte. Zeitschrift für die gesamte Versicherungswirtschaft, 1979, pp. 279-299.

[8] Müller, G, Eymann, T., and Kreutzer, M.: Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft. Oldenbourg, München, 2003.

[9] Müller, G., and Rannenberg, K.: Multilateral Security in Communications. Vol. 3: Technology, Infrastructure, Economy. Addison-Wesley-Longman, New York, 1999.

[10] Piaz, J.-M.: Operational Risk Management bei Banken. Versus-Verlag, Zürich, 2001.

[11] Rannenberg, K.: Zertifizierung Mehrseitiger Sicherheit: Kriterien und organisatorische Rahmenbedingungen. Vieweg, Braunschweig, Wiesbaden, 1998.

[12] Sackmann, S., and Strüker, J.: 10 Jahre E-Commerce – Eine stille Revolution in deutschen Unternehmen. Forthcoming (in german).