Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001

Wolfgang Boehmer
Technische Universität Darmstadt
Dep. of Computer Science, Research Group IT-Security
Hochschulstr. 10, D-64289 Darmstadt,
wboehmer@sec.informatik.tu-darmstadt.de

Abstract

The ISO27001:2005, as an information security management system (ISMS), is establishing itself more and more as the security standard in enterprises. In 2008 more than 4457 certified enterprises could be registered worldwide[1]*. Nevertheless, the registering an ISMS still says nothing about the quality and performance of its implementation. Therefore, in this article, a method for measuring the performance of the implementation and operation of an ISMS is presented.*

1 Introduction

The ISO 27001 emerged from the national standard BS7799-2 and has discussed by [23]. Alternatively, the further development of information security management (ISO 17799) according to the six sigma approach is discussed in the literature [2]. In [5], an open framework is developed for an enterprise-wide security management system. An extensive overview of technical, as well as organizational, aspects of the security of information can be taken from the article by [20]. The NIST addresses its paper [4] at managers and recommends a 7-stage process of development, divided into two major activities, to define suitable performance measurements.

The effectiveness and efficiency (economic efficiency) can be understood in terms of quality, and are supported by the CObiT controlling method. How both of these parameters are to be measured, however, it is not described in CObiT. Controlling processes and exam possibilities in general are described in CObiT. In this article, the concept of quality will be transferred on to the ISO 27001:2005.

[1] cp. http://www.iso27001certificates.com/ (accessed March 23, 2008)

The ISO/IEC 27001:2005 originated in close connection with the ISO 9001:2001. After the ISO 9001:2001, the business processes of an enterprise are described in general, however, they are not assessed nor weighted according to importance or criticality. This means that all processes are equally important and have the same criticality. This is where ISO 27001:2005 applies. In an ISMS according to ISO 27001:2005, those processes which contribute critically to the business success are especially treated. These processes can be also summarised under the concept of a value chain. These critical processes of the value chain are subjected to a particular processing by means of a risk analysis in the ISO 27001. In other words, an information security management system (ISMS) according to ISO 27001 is a management system for enterprise risks. When dealing with the recognised risks, risk decision (avoid, mitigate, transfer, accept) are met according to monetary criteria and suitable measures are planned, which require financial resources. [3] follows a similar approach. [21] also defines a direct relationship between the security of information and the security of business. Information security as new Paradigma in the enterprise protection philosophy is argued by [12].

This rest of this article is organized as follows. In the next section the structure of a process-oriented assessment system is described. In the third section, which contain the main focus of the article, we present a performance framework. The framework is defined by two KPIs. In the fourth section, the matrix of the key performance indicators is discussed. Hypothetical KPIs and their interpretations are discussed using the effectiveness/efficiency matrix. This article concludes with a short summary of the essential results and an outlook on further investigations.

2 Structure and definitions of an assessment system

As an accompaniment to an ISMS, a corresponding documentation must be described as a proof of the implementation of the controls (e.g. preventive, detective and corrective actions) for the purpose of a continuous improvement for an ISMS. Therefore the documentation in ISO 27001:2005 according to Clause 4 establishes a central point and is mandatory for an ISMS. In Clause 4 of ISO 27001:2005 four different hierarchical levels $(\lambda_1, \ldots, \lambda_4)$ are distinguished as Fig. 1 indicates. The uppermost level λ_1 has an effect on

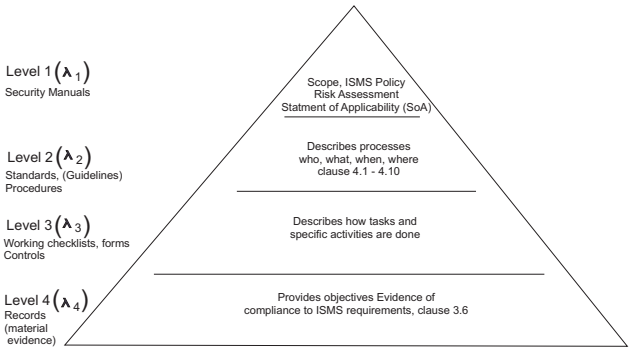

Fig. 1: Construction and power of a documentation of ISMS

the lower level, until, in the end, the last level λ_4 is reached. Therefore, Standards and Guidelines are required for the defined Policies assigned to the Lambda level. Standards and Guidelines are defined on the next lower level. Also Standards and Guidelines require procedures for enforcement. Procedures require check lists and working instructions. Then as a proof of the implementation, recordings exist on the last level (λ_4) in the form of protocols, log files and data. The triangular form in Fig. 1 represents the power of the incidental amounts of documents, recordings and proofs which increases from top to bottom.

2.1 Lower bound of effectiveness

Assuming both above-mentioned assessment dimensions, achievement indicators (P_λ) can be defined based on the structure of the ISMS documentation for every level (λ). The Fig.1 indicates that the number $\mathfrak{i}$ of the achievement indicators per level increases from the point (λ_1) up to base line (λ_4) using the triangular form. It still holds that the control variables are $\mathfrak{i}, \mathfrak{n}, \mathfrak{m}, \mathfrak{k}, \mathfrak{l} \in \mathbb{N}$ and that $\mathfrak{i} \leqslant \mathfrak{n} \leqslant \mathfrak{m} \leqslant \mathfrak{k} \leqslant \mathfrak{l}$. This lends the expression Eq.(1) to the stipulations according to the triangular form.

$$P_{\lambda_1}(\mathfrak{i}\ldots\mathfrak{n}) \leqslant P_{\lambda_2}(\mathfrak{i}\ldots\mathfrak{m}) \leqslant P_{\lambda_3}(\mathfrak{i}\ldots\mathfrak{k}) \leqslant P_{\lambda_4}(\mathfrak{i}\ldots\mathfrak{l}) \quad (1)$$

This means that, e.g., the number of security manuals (λ_1) and with it the number of the quantitative achievement indicators (P_{λ_1}) must be lower in an enterprise, than, e.g., the number of the quantitative achievement indicators (P_{λ_2}) of the procedures on the level (λ_2). Furthermore, it is postulated that $\mathfrak{n}, \mathfrak{m}, \mathfrak{k}, \mathfrak{l}$ must obey at least the following law and therefore fulfil the function of a lower bound. This critical success-factor (CFS) acts like a lower boundary towards an ISMS.

$$\mathfrak{m} = (2\mathfrak{n}+1)-\mathfrak{n}; \mathfrak{k} = (2\mathfrak{m}+1)-\mathfrak{n}; \mathfrak{l} = (2\mathfrak{k}+1)-\mathfrak{n} \quad (2)$$

Eq.(2) shows, for different $\mathfrak{n}$, how the lower boundary for four management indicators with restraints acts according to this law of generation.
This theoretical lower bound says, that an ISMS cannot be measured and it is outside of the assessment system when its effectiveness is located beneath this lower bound. However, the parameters refer to the first approximation, which is oriented on the hierarchical structure indicated by the documentation of the ISO 27001:2005.

Some examples for the key performance indicators (KPI) according to the Eq.(1) are listed in Tab. 1. Then, according to the quotient rule, further KPIs would have to be formed in close relation to the ISMS, depending on the numerical size of $\mathfrak{n}$. The consideration period of the indicators refers in each case to a fiscal year (Fy).

Tab. 1: Examples of key performance indicators at different levels

P_λ	Key Performance Indicators (KPI) per fiscal year
$P^{(1)}_{\lambda 1}$	Number of scope examination per year, related to the critical business processes
$P^{(2)}_{\lambda 1}$	Number of changes of critical assets per year
$P^{(3)}_{\lambda 1}$	Number of risk assessments per year
$P^{(1)}_{\lambda 2}$	Number of changes of the responsibilities
$P^{(2)}_{\lambda 2}$	Number of reviews for the security policies or/and procedures or/and checklists
$P^{(3)}_{\lambda 2}$	Number of preventive and corrective actions
$P^{(1)}_{\lambda 3}$	Number of changes within the controls
$P^{(2)}_{\lambda 3}$	Number of reviews of the checklists
$P^{(3)}_{\lambda 3}$	Number of reviews of the working instructions
$P^{(1)}_{\lambda 4}$	Number of changes within the risk acceptance
$P^{(2)}_{\lambda 4}$	Number of changes for the corrective and preventive actions
$P^{(3)}_{\lambda 4}$	Number of assessments to proof the validity of the key performance indications per year

Furthermore, the key performance indicators are in close connection with the statement of applicability (SOA). With

an increase in the controls which are addressed in the statement (SOA), the key performance indicators increase in the same manner. This connection can also be derived from the documentation requirements of an ISMS.

2.2 Upper bound of efficiency

A meaningful upper bound of efficiency arises from costs/benefit relation based on the risk decisions (e.g. avoid, mitigate, transfer, accept) for the critical business processes, as well as the controls deduced from them. R_G contains the number of all risks (whole risk). Based on this whole risk, some of the risks can be avoided (R_{av}), others are mitigated (R_{mi}) or, e.g., transferred to an insurer, or produced by outsourcing (R_{tr}). The residual risks (R_{ac}) are carried or accepted. The Eq.(3) shows the components of the whole risk.

$$\mathsf{R}_\mathsf{G} = \mathsf{R}_{av} + \mathsf{R}_{mi} + \mathsf{R}_{tr} + \mathsf{R}_{ac} \tag{3}$$

R_G has a monetary unit. A goal for every enterprise is to keep all costs for all controls (processes, tools, infrastructural controls), which are addressed in the SOA, lower than the costs (e.g., in EURO) that arise from the possible event of damage from R_{av}, R_{mi}, R_{tr}, R_{ac}. The Eq.(4) shows this relation.

$$SOA(€) \leqslant \mathsf{R}_\mathsf{G}(€) \tag{4}$$

Eq.(4) can be interpreted to the effect that no more expenses should be used for countering the risks than the value of the assets or the critical business processes of the value chain. A quite similar view is represented also by [22].

3 A performance framework for an ISMS

The demanded key performance indicators (KPI) and critical successful factors (CSF) can be understood as special key indicators. Key indicators numbers are based, according to [17] and [6], on empirical values from a concrete background and can be used to assess certain circumstances with only a few distinctive pieces of information. Essentially, one should begin with the identification of the critical business processes in case of an ISMS. If an ISMS is not aligned with the critical business processes, they can no longer reach the risks counter measurements correctly and gaps at all security levels (λ) could exist.

3.1 Appraisal of the effectiveness

In the case of the effectiveness with reference to an ISMS, some questions arise. These questions are aimed at securing the recognised risks and therefore also at counter measurements. The counter measures are motivated by suitable policies. Policies exist in several variations in an enterprise. Standards and guidelines are required to enforce these policies. From these standards and guidelines, procedures are created for enforcement [7]. Therefore, a special role is assigned to the policies of an ISMS with respect to the effectiveness.
Based on the following questions, an analysis of the effectiveness of the policies can be carried out in an enterprise:

- Do suitable and sufficient policies as well as procedures which refer to standards or guidelines exist and are these applied (degree or realisation)? A proof can take place, e.g., through internal or external audits.
- Have suitable and sufficient internal controls been arranged according to the existing policies (degree of enforcement)?
- Do suitable policies for the information security exist for all critical assets of the value added chain (degree of completeness)?

Policies can exist in very different forms, particularly in large companies (Entry level policies, Policies for special target groups, Topic related policies, Dynamic and static policies). In order to observe and preserve the (security) policies, examinations are necessary in the form of assessments through audits. The audits serve the purpose of checking the *internal controls*, consisting of preventive, detective and corrective activities. The purpose of the controls are to prevent harm and protect an asset. Internal controls can consist of administrative controls, physical controls, and technical controls. Moreover, different forms of an audit are found in the literature [14] and [7].
An assessment (*As*), within the scope of an audit, checks a series ($\mathtt{i}$) of checkpoints (*CP*) or processes, to see if these conform with the norm. Concrete suggestions for the realisation of an assessment can be found in the literature [16], [25] or also [14]. If some ($\mathtt{j}$) deviations is ascertained with an assessment, these deviations are reported in a special ISO 27001:2005 nonconformity report (*NoC*). Using this, a special key performance indicator (*US*) can be derived for the policies, standards and procedures in the results of an assessments (*As*) by the Eq.(5).

$$US = \frac{\sum_{\mathtt{i}=1}^{\mathtt{n}} CP_\mathtt{i} - \sum_{\mathtt{j}=1}^{\mathtt{m}} NoC_\mathtt{j}}{\sum_{\mathtt{i}=1}^{\mathtt{n}} CP_\mathtt{i}} \tag{5}$$

$\mathtt{i}, \mathtt{j}, \mathtt{n}, \mathtt{m} \in \mathbb{N}$ respectively. According to Eq.(5), the result is always between $0 \leqslant US \leqslant 1$ and can be interpreted as a degree of realisation.

Assessments in the form of internal or external audits can take place on the base of different documents (e.g. security manuals, procedures, working instructions, working checklists, forms and records). Two different test methods are to be distinguished, according to [7]: on the one hand, the

compliance testing method and on the other hand, the substantive testing method. Because, in general, several assessments (As) are carried out per level according to the number of different documents, the respective results can be added up and divided by the total number of assessments, so that we receive a degree of enforcement per level. Consequently, enforcement deficits at different levels can be identified.

The better one security manual is enforced, the more obligatory it's application becomes. The degree of enforcement should be designed as a correction factor for the degree of realisation like in Eq.(5).

In the ideal case, assessments are carried out for all existing security manuals on the basis of all documents linked with them. In each case, a suitable document hierarchy is in place. For every level we determine the values according to Eq.(6). The requirements which cannot be inspected on a higher level should be inspected at one of the lower levels. If no checkpoints are to be found, the requirements (security manuals) are not sufficiently enforced. These open or nonexistent checkpoints (*NoCP*) are, analogous to the Eq.(5), added up as *not operable*, subtracted from the total number of checkpoints (*CP*) and then set in relation to the total number of all checkpoints. In doing this, we receive, analogous to the degree of realisation, a KPI, which describes the degree of enforcement (*OP*) of the security policy *(SP)*.

$$OP = \frac{\sum_{i=1}^{n} CP_i - \sum_{j=1}^{m} NoCP_j}{\sum_{i=1}^{n} CP_i} \tag{6}$$

By multiplying both dimensions ($US \times OP$), we receive an indicator for the quality of the security policy (Quality of SP, *QoSP*). The immense importance of the security policy for the enterprise has also been worked out by [10].

A high realisation quality of the policies is, indeed, a necessary condition on the effectiveness of an ISMS, however, it is not a sufficient condition. To be sufficient, the key performance indicator of the completeness (V) of the security policy with reference to the critical assets must also be considered.

An ISMS is oriented on the information security controls of the critical business processes (*cBP*), which depend on the assets of the critical business processes. To identify the risk for these assets we deploy a risk analysis. The value and quantity of these assets (*Asts*) are direct input for the risk analysis, which is not directly specified in the ISO 27001:2005 itself. The importance of the relationship between an information management system and his assets has been recognised in early 1994 and has been modeled in [1].

If the quantity of the assets changes within the period under review, the critical business processes have also changed. According to ISO 27001:2005, the following subjects and objects belong to the assets: Key persons, contracts, application, software, images, etc. The completeness depends on the quality and frequency of the identification of critical business processes (*cBP*). This can be achieved for the most part through regular audits and independent external audits. The key performance indicator of Eq.(7) shows the connection of the (non-)existing policies (*NoSP*) to the critical assets (*Asts*) and the critical business processes (*cBP*).

$$V = \frac{\sum_{i}^{n} Asts(cBP)_i - \sum_{j}^{m} Asts(NoSP)_j}{\sum_{i}^{n} Asts(cBP)_i} \tag{7}$$

The KPI of the effectiveness (Efk_k) is a result of the multiplication of the KPIs of Eq.(5), Eq.(6), Eq.(7). The following Eq.(8) shows this relationship.

$$Efk_k = US \times OP \times V \tag{8}$$

With the KPI of the effectiveness (Efk_k) from Eq.(8) of an ISMS within organisation is between $0 \leqslant Efk_k \leqslant 1$, $Efk_k \in \mathbb{R}$.

3.2 Appraisal of the efficiency

A cost consideration of the security of information is discussed in the literature controversially. A lot of articles refer to the calculation of the expenditure for the security counter measurements in a Return of Security Investment (ROSI) investigation, often to the (perimeter) defensive techniques [19], [11], [18], [24] and [13]. A possible profit loss of the organisation is confronted with the protection for the assets of the IT. Then the result is an approximation between the costs of a successful attack and the security costs (counter measurements).

Other considerations in the literature deal with the profit loss, which is counted as a loss of productiveness, e.g., with the non-availability of a file server and hence a certain number of employees not can be active [22]. Furthermore, [22] explains that suitable material for a benchmark still does not exist.

The consideration of the profit loss is aimed at the increase of the operating expenses and at the influence of the business processes. This addresses another point in the consideration of the efficiency. However, when considered in isolation, these costs also only show one partial aspect in the efficiency of an ISMS.

In the article from [9], it is argued that a cost consideration could not be successful with the ROSI model. In [8], it is indicated that companies often apply a fear, uncertainty, and doubt (FUD) strategy for investments in the area of the security counter measurement. [24] gives a good overview of the different approaches to the ROSI model.

The consideration discussed above includes neither the indirect costs nor the operating expenses in the cost evaluations. In addition, the direct costs will only be partially

taken into account. From the point of view of the critical processes of an ISMS, the suggestions consider merely partial aspects. With the efficiency of an ISMS, the focus is on the efficiency (economic aspects) of the security counter measurements of the critical business processes or their assets. The economic efficiency is to be determined in principle as a costs/benefit relationship. To successfully plan for the budget of the critical processes for an enterprise, the infrastructure costs Eq.(10) as well as the costs to the risk defence must be considered (Eq.11, Eq.12, Eq.13).
A Total-Cost-of-Ownership model (TCO) provides an adequate look at the costs. In the TCO model, three cost drivers are identified. The sum of the direct costs ($\sum_i^n D_{C_i}$), and the indirect costs ($\sum_k^p I_{C_k}$) and of the operating expenses ($\sum_j^m O_{C_j}$) is to be mentioned.
At first glance, the TCO model seems to be sufficient for the interests of an ISMS when considering the infrastructure costs. The three cost categories mentioned can be defined as follows:

- Direct costs ($\sum_i^n D_{C_i}$): Employees, hardware, software, external services, physical environments (buildings, etc.) in which data processing should take place under secure conditions for an organisation. Moreover, in addition to the acquisition of the devices (security appliances), their resulting value consumption has to be calculated.
- Operating expenses ($\sum_j^m O_{C_j}$): Costs, that must be considered when calculating the maintenance, servicing, repair of the components listed as direct costs above.
- Indirect costs ($\sum_k^p I_{C_k}$): These expenses originate as a result of unproductive time from the end user.

The general TCO model would have to be adapted to the scope of an ISMS - to the critical processes. In addition, the TCO model would not have to be of static nature, in the interest of increasing efficiency, but be subject to a Demming cycle in accordance with ISO 9001:2001 .
As a modification, the TCO model, referencing a fiscal year, e.g., Fy_0, at t_0, could calculate the the costs based on the infrastructural controls of the critical business processes of an ISMS. With this, the infrastructural costs can be expressed for a fiscal year as follows for an ISMS:

$$Fy_0 = \sum_{i=1}^{n} D_{C_i} + \sum_{j=1}^{m} I_{C_j} + \sum_{k=1}^{p} O_{C_k} \tag{9}$$

Then a change (Iteration) can be calculated by one fiscal year (Fy_0), at t_0, referring to the next fiscal year (Fy_1), at t_1. Therefore the following connection arises for the cost change for the infrastructural controls of an ISMS:

$$TCO_{ISMS} = \frac{Fy_1 - Fy_0}{Fy_0} \tag{10}$$

Beside the infrastructure costs, the expenses are to be considered for the risk defence. An essential benefit of an ISMS is the aimed cost-contact with the recognized risks. A series of questions present themselves in order to define the the efficiency (economic) of the risk defence:

1. Which of the recognised risks out of all risks (R_G) can most likely be avoided under economic points of view (R_{av})?
   What are the costs of the controls (infrastructural expenses Eq.(9) and expenses of the risk avoidance Eq.(11)) in one fiscal year?
2. Which of the recognised risks out of all risks (R_G) can be most likely mitigated under economic aspects (R_{mi})?
   What are the costs of these controls (infrastructural expenses Eq.(9) and expenses of the risk avoidance Eq.(12)) in one fiscal year?
3. Which of the recognised risks out of all risks (R_G) can be most likely transferred under economic points of view (R_{tr})?
   What are the costs of the contracts Eq.(13) in one fiscal year? The infrastructural expenses Eq.(9) are omitted.
4. Which of the recognised risks out of all risks (R_G) can be most likely accepted under economic points of view(R_{ac})?
   No expenses arise for the infrastructure Eq.(9) and for the risk defence.

Four alternative actions can be described for these four questions to make different decisions. Formally this could take place with the help of the normative decision theory. Therefore, the expenses in accordance with the four alternative actions, $R_{1_{Cost}}$, $R_{2_{Cost}}$ and $R_{3_{Cost}}$ are as follows:

$$R_{1Cost} = R_1 = \sum_{i=1}^{n} R_{av_i} \tag{11}$$

Eq.(11) describes the expenses (R_{1Cost}) that were estimated for the avoidance of the risks.

$$R_{2Cost} = R_2 = \sum_{j=1}^{m} R_{mij} \tag{12}$$

Eq.(12) describes the expenses (R_{2Cost}) that were estimated for the mitigation of the risks.

$$R_{3Cost} = R_3 = \sum_{k=1}^{p} R_{trk} \tag{13}$$

Eq.(13) describes the expenses (R_{3Cost}) that were estimated for the transference of the risks. For the accepted risks (R_{ac}),

no expenses can be estimated, as long as these risks have not occurred.
In section 2 we defined an upper bound. This bound means that at least a cost balance according to Eq.(4) must exist. Otherwise the ISMS is pursued uneconomically. Nevertheless, this unique ascertained efficiency (economic) must be determined again each fiscal year (Fy).
For an ISMS, the whole risk ($\mathsf{R_G}$) can be derived, according to Eq.(3), from a risk analysis carried out in one fiscal year, e.g. ($\mathsf{Fy_0}$). According to Eq.(3) initiated controls in accordance with ISO 27002:2007 reduce the risk situation. This risk management is strictly carried out according to economic conditions. If a risk analysis is carried out in the next fiscal year again at the time of $\mathsf{Fy_1}$, a low risk situation arises as far as the damage reduction is concerned:

- The processes for avoiding risks can be optimised.
- The processes and controls for the mitigation of the risks can be optimised.
- The expenses for transferring the risks have changed (increased, decreased).

Out of this, a possible difference arises for $\mathsf{R_G}$, which is to be explained by a change in the cost of dealing with the risks (mitigation, avoiding, transfer, accepting).
It then follows, that for the KPI of the efficiency (Efz_k) can be understood as a economic component with reference to an interval (δt). Efz_k describe the comparison of two fiscal years ($\delta F \geqslant 0 = \mathsf{Fy_0} - \mathsf{Fy_1}$) for the expenses of the risk defense ($\mathsf{R_{1\,Cost}}$, $\mathsf{R_{2\,Cost}}$ and $\mathsf{R_{3\,Cost}}$) and the infrastructural expenses from Eq.(10).

$$Efz_k = \frac{\sum_{i=1}^{3} \mathsf{R_{i\,Cost}} + \mathsf{Fy_0} - \left(\sum_{i=1}^{3} \mathsf{R_{i\,Cost}} + \mathsf{Fy_1}\right)}{\sum_{i=1}^{3} \mathsf{R_{i\,Cost}} + \mathsf{Fy_0}} \quad (14)$$

Eq.(14) shows that $Efz_k \in \mathbb{R}$ could be a positive as well as a negative indicator. Nevertheless, it is postulated in Eq.(14) that in a fiscal year $\mathsf{Fy_1}$, less budget is required for risk defense than in the fiscal year $\mathsf{Fy_0}$. Therefore the key indicator is ordinarily positive. Otherwise, if more budget is given than in the year before, a negative indicator results.
In this section, it becomes clear that risk management corresponds to cost management and information security management (ISMS) based on ISO 27001 contains risk management.

3.3 Key performance matrix of the effectiveness and efficiency

To be able to determine the quality of an ISMS, the KPI of the effectiveness must be placed in relation to the efficiency. This takes both the efficiency (economic) and the effectiveness of an ISMS into equal consideration. Both key indicators show two properties that should be kept strictly separated qualitatively and also should not be aggregated to one single key indicator. The actual security counter measurements for the critical business processes and their efficient realisation can be shown in a matrix. Within the matrix, the KPIs of the effectiveness of the ISMS span the one axis and the key indicators of the efficiency span the other axis. The key performance indicators of the effectiveness and those of the efficiency move in each case between 0 $\leqslant Efk_k \leqslant 1$ and $-1 \leqslant Efz_k \leqslant 1$. The following can be defined as the first, arbitrary linear approximation for the effectiveness:

$$\mathsf{Efk_k} = \begin{cases} \mathsf{yes} & = & 0,5 < 1 \\ \mathsf{no} & = & 0 \leqslant 0,5 \end{cases} \quad (15)$$

If the key indicator crosses the value of 0.5, the ISMS moves in the positive area (yes). If the case arises that the key indicator is below 0.5, a (no) is assigned. A similar distinction can be defined for the key indicator of the efficiency:

$$\mathsf{Efz_k} = \begin{cases} \mathsf{yes} & = & 0 < 1 \\ \mathsf{no} & = & -1 \leqslant 0 \end{cases} \quad (16)$$

Presumably, in principle all possible combinations of the Eq.(15) and Eq.(16) become observable with suitable investigations in practice be. In the Fig. 2, these four cases (I, II, III, IV) are shown.
Case IV can be described as an ideal state of an ISMS.

Effective / Efficient	yes	no
yes	IV: ISMS is effective and efficient	I: ISMS is effective but not efficient
no	III: ISMS is not effective but efficient	II: ISMS is not effective nor efficient

Fig. 2: Performance matrix of an ISMS

IV: *ISMS is effective and efficient*
This case can be defined as a strategic balance: The operation of the safeguarding of the critical business process under the aspect of the efficiency is in a strategic balance. The operation of the security controls are completely efficient. The ISMS supports the IT strategy efficiently with the right security controls, while at the same time the security controls are marked by an optimum cost/ benefit relationship.

In addition to the strategic balance, three kinds of imbalance, as [15] defines, exist for an IMS[2]. Transferred on to

[2]IMS is the abbreviation for an information management system

an ISMS, which is done in Fig.2, this denotes that the cases I, II, and III are imbalanced for an ISMS:

I: *ISMS is effective but not efficient*
Corresponds to a strategic waste: This enterprise situation is marked by the fact that the effectiveness is high due to the operation of an information security management system, but efficiency has not been achieved. Indeed, the achievement potential of an ISMS is exhausted effectively, however, the exhaustion takes place uneconomically.

II: *ISMS is neither effective nor efficient*
Corresponds to a strategic dilemma: The operation of an ISMS, as well as its achievement potential are neither effective in the strategical dilemma, nor efficient. The achievement potential is barely exhausted, as are the effective security counter measurements for the critical business process in the enterprise, although considerable investments are effected in the area of information security. A dissipation as well as a waste of valuable resources exist.

III: *ISMS is not effective, but efficient*
Corresponds to a strategical dissipation: With the strategic dissipation, the efficiency of an ISMS is high, the effectiveness of an ISMS, however, very low. The achievement potential of an ISMS is not still properly recognised nor exhausted. Every control in the area of information security is considered typically unique and, hence, is often misjudged.

4 Conclusions and further investigations

In this article, we argued that KPIs of the effectiveness and the efficiency can measure the quality of an ISMS according to ISO 27001. Only one measurement can be carried out if a defined lower and upper bound is kept. Within these bounds, the performance can be measured. For the determination of the KPI of the effectiveness and the efficiency, several parameters have been defined. However, effectiveness and efficiency are strictly considered separately. The only thing they have in common is that the same consideration period has to be taken. As an ideal case, a strategic balance can be determined if the operation of the safeguarding is proved effective and the expenses for the controls in a fiscal year have decreased in the next fiscal year.

Moreover, with this article we also showed that an information security management system (ISMS) based on ISO 27001 is strongly related to a risk management and risk management is to be on par with cost management. It is planned to verify the four cases by empiric tests in practice.

References

[1] Anderson, A. et al.: Security Modeling for organisations; ACM, CCs 11/94 Fairfax Va., USA, ACM 0-89791-732-4/94/0011, p. 241-250.

[2] Bakry, S. H. et. al.: Using ISO 17799:2005 information security management: a STOPE view with six sigma approach; Int. J. Network Mgmt 2007;17: p. 85-97.

[3] Blakley, B. et. al.: Information Security is Information Risk Management; NSPW'01, September 10-13th, 2002, Cloudcroft, New Mexico, USA. ACM 1-58113-457-6/01/0009.

[4] Bowen, P.; Hash, J.; Wilson, M.: Information Security Handbook: A Guide for Manager, NIST Special Publication 800-100,Oct. 2006, Recommendatins of National Institute of Standards and Technology.

[5] Bradley, D. and Josang, A.: Mesmerize - an open framework for enterprise security management; AISW 2004, Dunedin, New Zealand, in Conferences in Research and Practice in Information Technology, Vol. 32, pages 37-42.

[6] Caralli, Richard, A.: The Critical Success Factor Method: Established a Foundation for Enterprise Security Management, Technical Report, Carnegie Mellon University, CMU/SEI-2004-TR-010, July 2004.

[7] Cannon L., et al.: Certified Information Systems Auditor; Wiley Publishing, Inc., Indianapolis, Indiana, ISBN-13:978-0-7821-4438-3, pages 49-82.

[8] Cavusolgu, H. et. al.: A Model For Evaluating IT Security Investment; Communication of the ACM, July 2004, Vol.47,. No. 7, p. 87-92.

[9] Davis, A.: Return on security investment – proving its worth it Network Security, Volume 2005, Issue 11, November 2005, pages 8-10.

[10] Doherty, N.; Fulford, H.: Aligning the information security policy with the strategic information systems plan; Elsevier, Computer & Security; 25 (2006), p. 55-63.

[11] Eloff, J. and Eloff M.: Information security architecture; Computer Fraud & Security; Nov. 2005, pages 10-16.

[12] Eloff, J.: Information Security Management - A new Paradigma; Proceedings of SAICSIT 2003, Pages 130-136.

[13] Gordon, L. and Loeb, M.: The Economics of Information Security Investment; ACM Trasaction on Information and Systems Security, Vol.5 No.4 Nov. 2002, pages 438-457.

[14] Gallegos F., et. al.: Information Technology Control and Audit - 2nd Edition; Auerbach Publishing, 2004, ISBN-13:9780849320323.

[15] Heinrich, L. et Lehner F.: Informationmanagement, Planung, Überwachung und Steuerung der Informationsinfrastruktur. 8 Auflage, Oldenbourg Verlag, München, 2005; p.84, ISBN-13:9783486577723.

[16] Kairab, S.: A Practical Guide to Security Assessments, Auerbach Publications, CRC Press, 2005, ISBN 0-8493-1706-1.

[17] Kütz, M.: IT-Controlling für die Praxis; dpunkt Verlag, 1. Auflage 2005, pages 44-45, ISBN 3-89864-265-8.

[18] Larochelle, D. and Rosasco, N.: Towards a Model of the Costs of Security, Technical Report CS-2003-13, June 2003. University of Virginia, Dept. of Computer Science.

[19] Mizzi, A.: Return of Information Security Investment, Are you spending enough? Are you spending too much? Available: http:/www.geocities/amz/ (accssed August 30, 2005).

[20] Siponen, M.: Information Security Standards Focus on the Existence of Process, not its content; Communication of the ACM, 2006/Vol.49, No.8.

[21] von Solms, B. and von Solms, R.: From information security to ... business security? Computer & Security (2005) 24, pages 271-273.

[22] Sonnenreich, W.: Return On Security Investment (ROSI): A Practical Quantitative Model, SageSecure, LLC.; Available: http:www.infosecwriters.com/textresources/pdf/ROSI-PracticalModel.pdf (accssed April 20, 2008)

[23] Tong C., et. al.: Implementation of ISO17799 and BS7799 in picture archiving and communications system: local experience in implementation of BS7799 Standard. CARS 2003:London UK, pages 311-318.

[24] Tsiakis, T. and Stephanides G.: The economic approach of information security Computers & Security, Volume 24, Issue 2, March 2005, Pages 105-108.

[25] Wescott, R.: Maximizing the ROI of a security audit Network Security, Volume 2007, Issue 3, March 2007, Pages 8-11