Performance, survivability, and cost aspects of Business Continuity Processes According to BS 25999

Wolfgang Boehmer*
*Technische Universitaet Darmstadt, Germany, Hochschulstr. 10, 64289 Darmstadt
Email: wboehmer@cdc.informatik.tu-darmstadt.de

***Abstract*—A new model is presented for evaluating the performance of a Business Continuity Management System according to BS 25999. Performance is based fundamentally on the system's Business Continuity Plans and Disaster Recovery Plans. Typically, the performance of these plans is inadequately evaluated using a number of specific exercises at various intervals and, in many cases, with a variety of targets. Consequently, it is difficult for companies to give *ex-ante* statements of their survival in the case of a disaster.**

Two key performance indicators are presented that allow the performance of a Business Continuity Management System to be evaluated according to BS 25999. Using these key performance indicators, the probability of survival can be estimated before extreme events occur. However, the two key performance indicators compete and their use invokes a trade-off: an alignment in favor of one key performance indicator is necessarily done at the expense of the other. A key performance matrix with four ranges is presented according to the Business Continuity Management System. The best range is the strategic balance in which both key performance indicators support the economic strategy and a suitable cost/benefit relationship is achieved. Moreover, if a company is already in the range of the strategic balance, a further improvement, which yields minimal turnover, may be possible. This improvement can be obtained via a combinatorial optimization between the two competing key performance indicators.

***Index Terms*—BS 25999; BCMS; Business Continuity Plan (BCP); Knapsack-Problem; Branch & Bounding.**

I. Introduction

This contribution is inspired by [1] which addresses measurement of performance indicators for effectiveness and economic efficiency of a Business Continuity Management System (BCMS). However, in this article the evolution of key performance indicators is interpreted as a trade-off between the conflicting goals of effectiveness and economic efficiency. This trade-off is analogous to a 0-1 knapsack problem. Furthermore, it is proposed that a management system (BCMS) can be interpreted as a control loop with a steady state based on systems theory for Discrete Event Systems (DEVS). If this interpretation is acceptable, then DEVS knowledge can be transferred to a management system.

The BS 25999-1:2006 standard sets out the code of practice for a BCMS [2]. After extensive review by the British Standard Institution (BSI), specifications for Business Continuity Management (BCM), BS 25999-2:2007, were published in November 2007 [3]. During that review, more than 5000 industrial ideas and suggestions were integrated into the standard, thereby establishing a high level of maturity. The standard BS 25999-2:2007 provides requirements that a management system must meet if critical business processes (value chain) are to remain stable in the face of acceptable levels of disasters. The fundamental idea is that BCM aims to manage various types of uncommon business risks that would have a huge impact on a company. A BCMS is capable of responding satisfactorily in extreme situations (catastrophic events) with pre-defined plans (Business Continuity Plans; BCP). The continuation of the value chain at an acceptable level for a defined period (Δt) is then ensured. A BCMS includes vital business processes. Recovering only the working infrastructure, e.g., replacing a failed IT infrastructure by an emergency one, will not meet a BCMS, as an IBM report clearly points out [4].

The BS 25999 standard requires implementation of a management system in accordance with the PDCA cycle (Plan–Do–Check–Act) as well as those systems already required in other standards, such as ISO/IEC 27001, ISO/IEC 20000, ISO/IEC 9001, and ISO/IEC14001. However, those standards describe only *what* to do rather than *how* to do it.

The PDCA[1] cycle is based on the idea of imperfection and thus follows a continuous improvement process. For example, in the Check phase, managers examine whether the plan's objective set is still in agreement with the rest of the system. If it is not, corrections are implemented in the Act stage.

During the initial Plan phase of a PDCA cycle, BS 25999 requires identification of critical business processes and analysis of dependencies between key stakeholders and key services. Following this, a risk analysis must be performed. For each risk of high impact and low probability, a response [i.e., a Business Continuity Plan (BCP)] must be developed. The response is aimed, on the one hand, at continuing business processes on a defined level (BCPs) and, on the other, at initiating those countermeasures that will restore the original state (Disaster Recovery Plan, DRP).

As in the ISO 27001 standard, risk plays a central role in BS 25999 [5][3]. However, the measures for implementing ISO 27001 are oriented toward risk-prevention, while those for BS 25999 (BCP and DRP) are reactive. That is, BCM is a reactive model that becomes active only after a disaster has occurred.

[1]The PDCA cycle was developed by W. E. Deming in the late 60s of the last century.

In this context, the maximum allowable downtime (Maximum Tolerable Period of Disruption; MTPD), which starts after a disaster occurs, increases considerably in importance. The MTPD is determined from the length of time that critical activities in the value chain require to begin working again after a disaster. This period of time is an ultimate boundary for a company and decides the company's survival. If this ultimate limit is exceeded, the company is irretrievably lost. Consequently, the goal of every company must be to optimize the performance of the restoration so that the time required for restoration (Recovery Time of Objective; RTO) is reduced. Thus, a company must do everything to ensure that RTO $\leq$ MTPD can be achieved. However, the efficiency of restoration measures must not be ignored.

The relation between critical activities and the value chain is determined by the Business Impact Analysis (BIA). Within the BIA, the dependent critical resources (key stakeholders, key products, key services) and their importance to critical activities (core processes of the value chain) are analyzed. Any BCMS includes those business processes that are vital. A BCMS is capable of responding satisfactorily in extreme situations (catastrophic events) with pre-defined plans and emergency processes (Business Continuity Processes, BCP). This raises the question as to how well the performance of emergency processes are. However, performance, as in CobiT and in ISO/IEC 9004:2009, is also understood here [6].

In the literature, three basic methods are generally available for measuring the performance of processes.

1) It one method, performance is related to the maturity of processes, and tools such as Spice (ISO/IEC 15504) or CMMI, developed at Carnegie Mellon University, are used to measure process maturity. This maturity approach is gaining support across a wide range of technical environments, including production environments as well as management systems such as ITIL (ISO/IEC 20000) and ISO/IEC 27001.
2) A somewhat newer method is to describe the state space of processes using process algebra. In the development carried out at the TU Eindhoven, classical process algebra was not used, but a tool (mcrl2) has been developed by which process algebra can be applied in a simple manner. Then, if modal logic is applied in the form of a μcalculus on the state-space, the process algebra generated by state sequences and state transitions of all processes allows safety issues and the liveness of processes to be analyzed. Essentially, model checking is performed based on a specification. First thoughts were published in [7] and a study of this method applied to a business continuity process (BCP) has been published [8]. An extensive explanation can be found in the Technical Report of the TU Eindhoven [9]. Note that this method is distinct from symbolic model verification (SMV) used in such tools as νSMV and SMV.
3) Another method is to estimate performance on the basis of appropriate indicators (KPI). The challenge is to define appropriate metrics, which have a corresponding significance. Suggestions for the handling of such indicators are to be found in [10] and in [11]. A performance measurement system for a BCMS is developed in [12]. It rests upon the methodology of the BORIS, which contains a set of different tools. In that article, traditional security variables (integrity, availability, confidentiality) and business indicators, appear to be necessary [12]. A similar approach to a performance measurement system has been applied in [1] for business continuity management (BCM) and a forerunner of this approach was published in [13].

In a previous article by Boehmer, it was demonstrated how the management system of ISO 27001 can be measured using effectiveness and efficiency as indicators [13]. As mentioned above, a measurement takes place in the Check phase. In the present paper, this idea of measuring the quality of these two KPIs is applied to a BCMS. Measurements of these KPIs provide the status of a BCMS; that status maps into one of four quadrants. The worst state is one in which a BCMS is neither effective nor efficient; this is called a strategic dilemma [13]. In a strategic dilemma, the probability of a catastrophe occurring in which the company will not survive is very high. Conversely, the survival probability increases if the ratio of the effectiveness and efficiency of the KPI is ideal and the majority of all the exercises carried out has $RTO \leq MTPD$.

This paper is divided into seven sections. The following section integrates relevant work from the literature. The third section contains a discussion of the structure of a process-oriented evaluation system based on circumstantial evidence and key indicators. In the fourth section, the development of two KPIs is discussed; these KPIs are used in the fifth section to look at survival probability. Survival probability is closely linked to a functioning BCP. In the sixth section trade-offs between the KPIs of effectiveness and efficiency are discussed within the context of the 0-1 knapsack problem. Our contribution finishes with a brief summary and prospects for future work.

II. Related Work

An empirical study by Knight and Pretty shows that those companies with a BCMS are more likely to survive a disaster than those that have taken no precautions [14]. Nevertheless, the study also shows that, despite the use of a BCMS, a company's chance of survival is not guaranteed, and a small number of such companies have been reported as failing to survive. Conversely, the study also reports a very small number of companies that survived a disaster even though they had no BCMS [14]. This latter phenomenon may simply be luck.

Looking at those cases of companies that used a BCMS and still did not survive, it appears the quality of their BCMS or BCP and DRP needs to be taken into account. It is clear from the study that the application of a standard is not, by itself, enough: the standard must be applied properly.

The literature has so far focused on the topic of BCMS primarily in practical terms, e.g., [15],[16],[17]. Nemzow discusses the need for various strategies to protect an organization

from natural and manmade disasters [15]. He also explains the difference between a BCP and a DRP. Quirchmayr discusses the Business Continuity Management Lifecycle and its content [16]. Landry and Koger discuss the lessons learned from 2005's hurricane Katrina [17]. Again, the importance of a DRP is stressed. Similar ideas are set out in the study by IBM on hurricane Katrina, including claims that a BCP and DRP must contain more than simple aspects of the company. For example, company members remaining in the disaster area should also be taken into account in the BCP [4]. Similarly, Saleem et al. [18] note the importance of an adequate Business Continuity Information Network on an effective DRP. A similar issue is also highlighted by Shklovski et al. [19]. The importance of a Business Impact Analysis (BIA) and the restoration point of objective after a disaster is discussed by Quirchmayr et al. [20]. These issues are related to the MTPD. Meanwhile, many of these aspects influenced the BS 25999-2:2007.

However, solely from the results of Knight and Pretty, a more detailed review can be posited [14]. This review must relate to a BCMS as well as to the function and performance of its BCP and DRP. Only after the quality of performance has been measured can a statement be made concerning a business's survival probability.

III. Business Continuity Managment System (BCMS)

The fundamental idea of a BCMS is that Business Continuity Management (BCM) is meant to manage those rare business risks that can have a huge impact on a company. The BCMS is capable of responding adequately in extreme situations (catastrophic events) with pre-defined plans (BCP). In the next section, the goal of a management system is discussed using a simple example, then this goal is transferred to a BCMS.

A. Concrete example–a weight management system

A simple real-world example is used here to illustrate the concept of a management system. Consider a person who wants to manage his or her weight using a management system that focusses on consumed and burned calories. A possible objective could be to balance these values, as illustrated in Figure 1. Another objective could be to reduce the weight of a person. In this case more calories must be burned than consumed. The measuring instrument is the weighing machine (scales). The ideal state is maintained by burning as many calories as are consumed. Then the system is in a dynamic equilibrium and energetic costs are balanced. Equilibrium is a state of a system that does not change with respect to one or more state variables over some period of time; i.e., on average, the weight remains constant over a long period.

In Figure 2 the weight management system is interpreted as a feedback system. Every time the person diverges from the ideal weight, an adjustment is made by the actuator (calories are burned). This behavior of the weight management system can be interpreted as a linear feedback system. This linear feedback system can be described with a Discrete Event

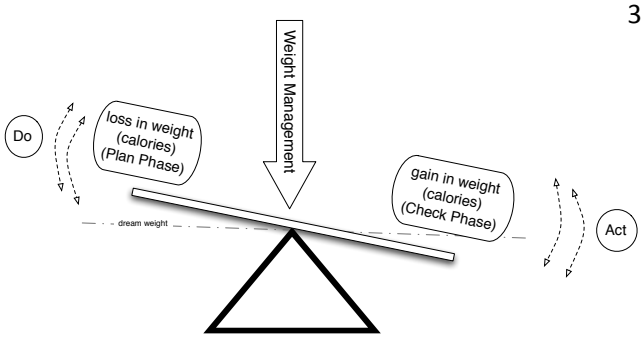

Fig. 1: Weight management system attempts to control gains and losses in a person's weight

System Specification (DEVS); it is a control loop that contains sensors (s), controller (c) and actuators (a) arranged to regulate in discrete (k)-steps a process variable (p) with respect to a reference signal $w(k)$ (see Figure 2).

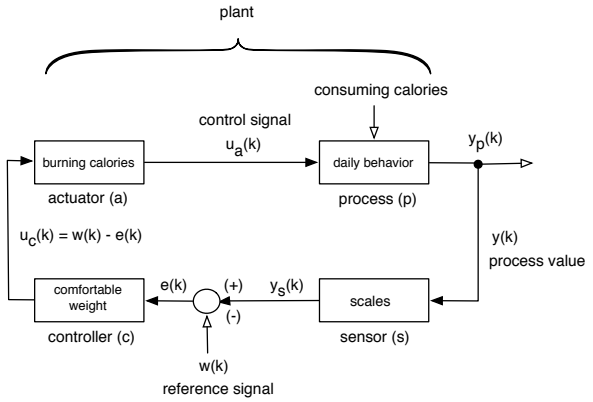

Fig. 2: Weight management system reinterpreted as a control loop for the weight of a person

The basic objective is to control the value of the process variable $y_p(k)$. This is done by measuring its value $y(k)$ and determining $e(k)$ its variance $(+/-)$ relative to the desired reference value $w(k)$. This variance $u_c = w(k) - e(k)$ is used by the actuator to generate an appropriate correcting control signal $u_a(k)$ that modifies the system's behavior and changes the value of $y_p(k)$ appropriately. A closed loop is created by the feedback of the controlled variable to the sensor and its conversion to a control signal, as in Figure 2.

Inside an atomic DEVS, an arbitrary formalism can be used. A DEVS can be viewed as a framework that unifies a number of other formalisms in a consistent, systems theoretic, state-centered fashion. Discrete Event System Specifications (DEVS) are dynamic systems whose state changes serve as a basis for discrete events.

A similar behavior is achieved through the PDCA cycle in a Business Continuity Management System (BCMS). As mentioned above, a PDCA cycle is based on imperfection and follows a continuous improvement process. The controlled

variables are the KPIs related to the effectiveness and efficiency of a business continuity process (BCP). The reference signal is the balance (equilibrium) between effectiveness and efficiency of each business continuity process (BCP) and each Diaster Recovery Process (DRP).

The PDCA cycle can be applied to each element of the BCMS; this results in a PDCA cycle for the BCP and DRP as well as for the BCMS itself. In Figure 3 a PDCA cycle is

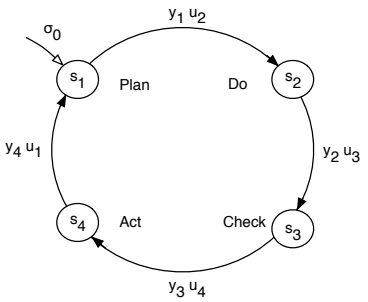

Fig. 3: PDCA cycle as a DEVS

modeled as a discrete deterministic finite automaton ($\mathcal{A}$). In this representation, the finite automaton can be defined as a 6-tuple,

$$\mathcal{A}(S, U, Y, \delta, g, s(0)) \tag{1}$$

Three finite sets occur:

$$S = \{s_1, ..., s_n\}\,; \text{ set of states} \tag{2}$$

$$U = \{u_1, ..., u_n\}\,; \text{ set of input alphabet} \tag{3}$$

$$Y = \{y_1, ..., y_n\}\,; \text{ set of output alphabet} \tag{4}$$

with two functions:

$$\delta : S \times U \longrightarrow S\,; \text{ transition function} \tag{5}$$

$$g : S \times U \longrightarrow Y; \text{ output function} \tag{6}$$

Furthermore, the initial state is called $s(0) \in S$. A single state is determined by $s \in S$, and its successor state s' is formed with the help of a transition function δ by $s' = \delta(s, u)$.

The four states in Figure 3 can be identified in accordance with BS 25999:

s_1= establishing and managing
s_2= implementing and operating
s_3= monitoring and reviewing
s_4= maintaining and improving

The state transition function is δ, k is the time independent counter, and g is the output function[2]. The automaton equations are then

$$s(k+1) = \delta(s(k), u(k))\ k = 0, 1, ... \tag{7}$$

$$y(k) = g(s(k), u(k))\ k = 0, 1, ... \tag{8}$$

Therefore an automaton ($\mathcal{A}$) is generated by an infinite state sequence and modeled by the continuous improvement of the PDCA cycle. If, after a certain time, alterations in the state no longer occur, so that a state change $(k+1)$ leaves the system in the old state with $s = y(s)$, then the state is an equilibrium one. This equilibrium condition expresses the balance between effectiveness and efficiency in the events of a BCMS for a BCP and DRP. In this case δ' is an extended state transition function for all absorbing states[3]. This condition is called a state of equilibrium [21].

Therefore, a BCMS with inherent PDCA cycles can be described with the system theory of discrete-event systems. States in the PDCA cycle for a BCP and DRP are measured by two key indicators, Efk and Efz. It is important to distinguish between an indicator and a key indicator. In the next section we show how this approach can be mapped onto the concept of a Business Continuity Management System.

B. Basic idea of a BCMS according BS 25999

A company that wants to safeguard its critical value chain should focus on securing revenues by taking adequate risk countermeasures. Since 2007, the BS 25999-2:2007 [3], published by the British Standard Institution (BSI), is available. It is an industry-wide recognized best-practice method that governs the creation of a BCMS. It encompasses a BCP and a DRP (Disaster Recovery Plan). The standard requires implementation of a management system in accordance with the PDCA cycle (Plan-Do-Check-Act), as well as those already required in standards ISO 27001, ISO 20000, and others.

Figure 4 illustrates the operational view of a PDCA cycle within an underlying BCMS. A BCMS is a framework that helps balance risks (potential disasters and impacts on the critical business process) against available countermeasures (business continuity processes and business recovery processes) while recognizing the MTPD as a real-world side constraint.

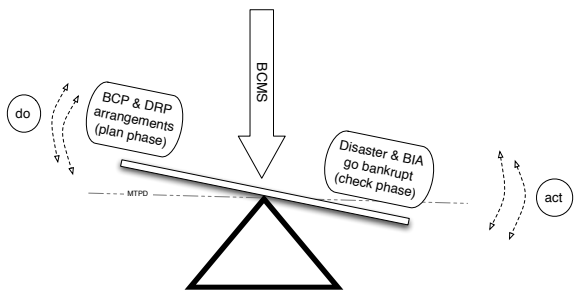

Fig. 4: Business Continuity Management System (BCMS) with ups and downs as a seesaw

Figure 5 shows a qualitative timeline of events following a disaster that strikes at time t_0. Immediately after occurrence of the disaster, turnover collapses. At time t_1 the processes of the BCP (emergency operation) begin, and turnover starts to increase. A little later, at time t_2, recovery processes start, and

[2]For more details we refer to the literature [21]

[3]Absorbing states are states that do not have successor states, and can be considered as final states.

at time t_4 the company is back to its normal level of operation. The dash dotted line in the figure shows the increase in costs after the disaster. In the event that no countermeasures (BCP, DRP) are taken, or that the countermeasures do not work, the costs continue to increase (see curve 2). The ideal situation is that the Business Continuity Plan and the Disaster Recovery Plan work so well that costs remain bounded, as in curve 1.

If no action (BCP, DRP) has been taken at or before the time t_3 in Figure 5, then costs will increase until insolvency is reached. Costs are determined by the obligations of the company. These consist of personnel, technical expenses, and the cost of delivery, performance, or possibly storage costs, etc. Thus t_3 identifies the maximum allowable downtime (Maximum Tolerable Period of Disruption; MTPD), $\Delta T_{max} = t_0 - t_3$.

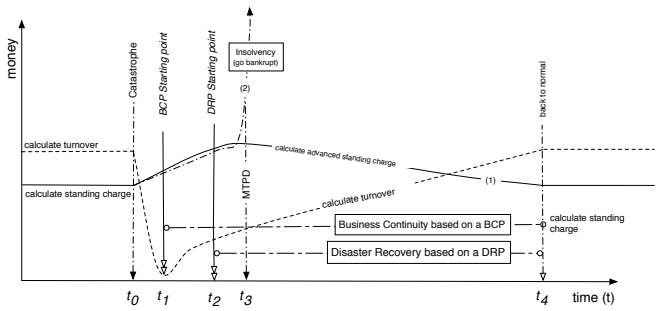

Fig. 5: Illustration of aspects of a catastrophe (t_0) and the reaction ($t_1, ..., t_4$)

It is in the self interest of a company to keep the BCPs and DRPs operational. Usually, this is tested on a regular basis by simulating that something goes astray within the ordinary business process. Because these tests are expensive, they are not executed very often and generally they only address certain aspects of the recovery plans. Such testing provides a rather haphazard prediction of the effectiveness of recovery plans when a true disaster strikes. To improve the quality of the analysis of BCPs and DRPs, one should model these and the ordinary business process such that they can be simulated. The first ideas of how to do this have been presented in [7].

IV. Performance Indicator of a BCMS according to BS 25999

This section shows how the key indicators of effectiveness and economic efficiency are developed. The controlled variables are the KPIs related to the effectiveness and efficiency of a business continuity process (BCP). The reference signal is the balance (equilibrium) between effectiveness and efficiency of each business continuity process (BCP) and each Diaster Recovery Process (DRP). In Figure 6 we see how a BCMS acts as a control loop, but to measure the performance of a BCP and a DRP, a number of indicators are required.

A number of indicators will be formed for each key indicator. An indicator and a key indicator can be defined as follows:

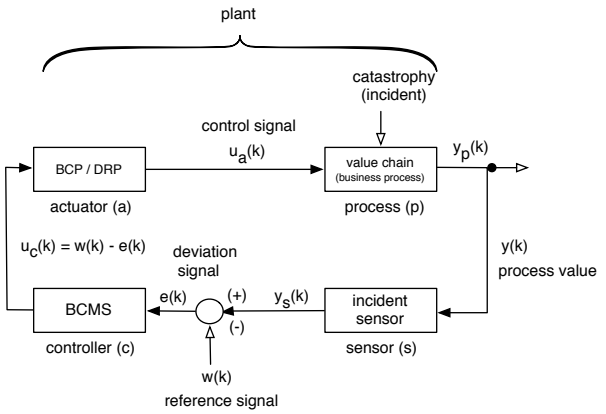

Fig. 6: BCMS Control loop for the emergency processes

Def. 1: An indicator (I) is a variable subject to a metric.

Def. 2: A Key Performance Indicator (KPI) is a key indicator formed from several more general indicators and provides a significant statement about a certain set of circumstances (see Eq. 18 and Eq. 22).

It is possible to make a significant statement using a key indicator, but this statement is supported by several more general indicators. The quality of a BCMS is reflected in the preparation, handling, and testing of the BCP and DRP in the Check phase (see Figure 4). For the system's effectiveness, this means that the indicator's

- existence (I_{ex}),
- enforcement (I_{op}) and
- completeness (I_{co})

form a set on the system effectiveness (Efk):

$$Efk = \{I_{ex}, I_{op_{(BCP,DRP)}}, I_{co}\}. \quad (9)$$

These indicators are derived about $\lambda_1, ..., \lambda_4$ from the pyramid-level documents (see Figure 7). This pyramid structure was derived by Alan Calder from practical experience and published in the ISMS Toolkit [22].

For the assessment system, performance values (KPI) can be defined for a BCMS. The documentation required by the standard plays a crucial role. From the required documentation, success measurements can be derived, and a lower boundary can be defined for the implementation of a BCMS. Below this boundary, a BCMS is inadequately implemented, and the effectiveness *(are we doing the right things?)* cannot be measured. Furthermore, an upper boundary is defined by the economic efficiency of the BCMS *(are we doing things right?)*. This consists of a cost/benefit relationship and follows the standard requirement (Clause 2.1.4 of the standard). This limit postulates that no more than the value of the critical business process should be invested in countermeasures.

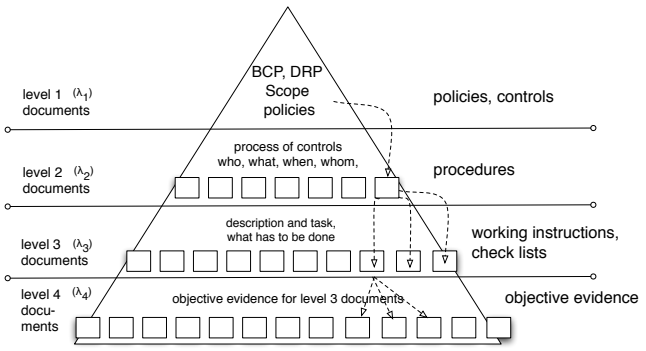

Fig. 7: Pyramid-level documents of a BCP and DRP

Figure 7 shows how the volume of documents from the top (λ_1) (peak) down increase. This structure shows the natural history based on a directive toward their technical implementation (procedures (λ_2), checklists (λ_3)), which provides a series of activities for implementing the directive. At the lowest level (λ_4) is the evidence *(objective evidence*), as described by Alan Calder [22]. This pyramid structure is now a condition for the existence of a lower boundary, as recommended in [13]. Below this boundary, the implementation of the management systems is not measurable. If the lower limit is exceeded, the quality of the BCMS and BRP and DRP can be measured on the basis of indicators.

The first key performance indicator (KPI_1) relates to the effectiveness (see Eq. 9) and can be determined by three indicators. On the one hand, the existence of the policies per BCP (Business Continuity Plan) can be evaluated with indicator I_{ex}. On the other hand, the degree of enforcement of policies is considered using indicator I_{op} relative to the BCP and DRP. Completeness (coverage) will be used as the third indicator, I_{co}. This indicates the coverage of the BIA as compared with the resources in relation to the scope of the BCMS.

The indicator I_{ex} evaluates the existence of control points (checkpoints; CP) or non-existent control points (NoCP) relative to a BCMS, according to BS 25999. The clauses of BS 25999 applied in the BCMS should be proven with control points; otherwise, no statement can be made about implementation of the standards. This case of the existence or non-existence of control points per document level ($\lambda_1, ..., \lambda_4$) can be expressed as

$$I_{ex} = \frac{\sum_{i=1}^{n} CP_{\lambda l} - \sum_{j=1}^{m} NoCP_{j(BCP)}}{\sum_{i=1}^{n} CP_{\lambda l}} \tag{10}$$

Thus, the indicator of control points I_{ex} is on the range between 0 and 1:

$$I_{ex} = \begin{cases} 1, & if\ NoCP = 0 \\ 0, & if\ \forall\ CP_{\lambda l} = 0; l = \{1,2,3,4\} \\ otherwise. \end{cases} \tag{11}$$

For ideal implementation of each standard in a business, the indicator should satisfy $I_{ex} \approx 1$ for each standard. This means that there are no deviations ($NoCP \approx 0$) between the control points (clauses) of the standards and the actual existing control points. When $I_{ex} \ll 1$, too few of the standard clauses have been applied and optimization is needed.

The existence of policies says little about whether they are actually present or whether they exist only on paper. Thus, Eq. 11 is a necessary but insufficient condition. This is precisely where the indicator of the degree of enforcement ($I_{op_{(BCP)}}, I_{op_{(DRP)}}$) is applied.

The indicator of the degree of enforcement ($I_{op_{(BCP)}}$) is based on the result of BCP Assessments, practical exercises, and deviations from the planned controls. For a BCP, the nonexistent measures ($NoC_{j(BCP)}$) are related to the necessary measures ($C_{\lambda l(BCP)}$) relative to the pyramid-level documents (see Figure 7). Whether adequate controls for a particular risk scenario are available for the continuation of critical business processes is determined. For each identified risk to critical business processes, there is a BCP and DRP. Here, the risk scenarios could be completely different. For example, a BCP and DRP for the risk of a pandemic scenario looks quite different than a scenario for the risk that a major supplier *(key stakeholder)* fails unexpectedly.

The indicator of the degree of enforcement ($I_{op_{(BCP)}}$) per document level (Eq. 12) checks the extent of discrepancies in the assessments between the action in BCP ($C_{\lambda l(BCP)}$) and the actual sequence ($NoC_{j(BCP)}$) in an exercise,

$$I_{op_{(BCP)}} = \frac{\sum_{i=1}^{n} C_{\lambda l(BCP)} - \sum_{j=1}^{m} NoC_{j(BCP)}}{\sum_{i=1}^{n} C_{\lambda l(BCP)}} \tag{12}$$

Thus, the indicator of the control points $I_{op_{(BCP)}}$ is on the range between 0 and 1 and is analogous to Eq. 11,

$$I_{op_{(BCP)}} = \begin{cases} 1, & if\ NoC_{(BCP)} = 0 \\ 0, & if\ \forall\ C_{\lambda l(BCP)} = 0; l = \{1,2,3,4\} \\ otherwise. \end{cases} \tag{13}$$

The BCP and DRP are closely linked to the standard but must be considered separately to allow for a granular approach. The indicator of the degree of enforcement ($I_{op_{(DRP)}}$) with relation to the DRP is based on the results from the assessments or exercises and the deviations ($NoC_{j(DRP)}$) of the proposed DRP ($C_{\lambda l(DRP)}$) controls,

$$I_{op_{(DRP)}} = \frac{\sum_{i=1}^{n} C_{\lambda l(DRP)} - \sum_{j=1}^{m} NoC_{j(DRP)}}{\sum_{i=1}^{n} C_{\lambda l(DRP)}} \tag{14}$$

Thus, the indicator of the control points $I_{op_{(DRP)}}$ is on the range between 0 and 1 and is analogous to Eq. 11. This indicator assesses the difference between planned activities and actual exercises,

$$I_{op_{(DRP)}} = \begin{cases} 1, & if\ NoC_{(DRP)} = 0 \\ 0, & if\ \forall\ C_{\lambda l(DRP)} = 0; l = \{1,2,3,4\} \\ otherwise. \end{cases} \tag{15}$$

Equation 15 ensures that the value of the practical experience gained during exercises for disaster recovery is recognized.

Key to effectiveness is the question of whether in fact all critical business processes in terms of resources have been considered with a BIA in relation to the scope of the BCMS. This observation is carried out using the indicator to assess coverage. The indicator (I_{co}) of the coverage of a BIA in relation to resources (key products, stakeholders, etc) within the scope leads to

$$I_{co} = \frac{\sum_{i=1}^{n} Res_{i(BIA)} - \sum_{j=1}^{m} Res_{j(NoSP)}}{\sum_{i=1}^{n} Res_{i(BIA)}} \tag{16}$$

Equation 16 places the critical resources (Res) within the BIA that must be treated with non-existing policies ($NoSP$) in relation to resources,

$$I_{co} = \begin{cases} 1, & if\ Res_{(NoSP)} = 0 \\ 0, & if\ \forall\ Res_{(BIA)} = 0 \\ otherwise. \end{cases} \tag{17}$$

Thus, the indicator (I_{co}) is on the range between 0 and 1 and is analogous to Eq. 11. The fewer the number of analyses that are present (BIA) for the critical resources, the smaller the coverage of the $I_{co} \ll 1$ critical processes, and the lower the effectiveness.

Finally, the indicators of effectiveness can be calculated with

$$Efk = I_{ex} \times I_{op_{(BCP)}} \times I_{op_{(DRP)}} \times I_{co} \tag{18}$$

This indicator (Efk) fluctuates between 0 and 1 and represents a point in a specific space spanned by the indicators. This key indicator says something about the effectiveness of the BCMS and the quality of the BCP and DRP. It provides a significant statement about a situation on the basis of the underlying indicators. Furthermore, Efk satisfies Def. 2 and is a key performance indicator for a company.

If the indicator is determined by numerous exercises and at a regular time interval t_0 and t_3 (see Figure 5), a conclusion may be drawn about the likelihood of survival in the event of a disaster. This aspect is discussed in the next section.

V. Estimation of the Survivability of a Business

In this section, the survival probability of a business is discussed. It is assumed that the business has implemented a BCMS in accordance with BS 25999 and that the indicators of effectiveness Efk and economic efficiency Efz have been identified. However, when economic efficiency is considered in advance (preventive or reactive controls) of a balance of controls, the indicator Efz is not used to consider the likelihood of survival.

After a disaster, the likelihood of survival of an enterprise is determined by the ratio of effectiveness. The effectiveness (Efk) can be understood as a random variable X in the interval *(a,b)* (see Figure 8). Figure 8 shows only the part between t_0 and t_3 (cf. Figure 5). Here, *(a)* can be identified as the entry point at the time of a disaster and then *(b)* is the date defined by the MTPD. Figure 8 relates the interval *(a,b)* to time ($a = t_0, b = t_3$). If the two markers *(a=1, b=0)* are set, the result of (x) lies in this interval if the exercises (assessments) of the BCP and DRP are used and an exercise gives a result of (x). If ($x = 1$) in the ideal case, then (t_0) and (t_1) almost coincide and the starting point of the BCP is immediately after the occurrence of the disaster. The reverse is also true: the smaller ($x \ll 1$) is, the longer before time (t_1) occurs, and the later the starting point of the BCP. If ($t_1 \geq t_3 = MTPD$), the business is irretrievable.

If there are enough exercises and assessments of the BCP and DRP, so that the effectiveness (Efk) can be measured and projected onto the interval *(a,b)*, the probability $P(a \leq X \leq b)$ for the interval $a \leq X \leq b$ can be given, where X takes on a value from the interval. Then, the likelihood function of the random variable X is known. Thus, the distribution function $F(x) = P(X \leq x)$ can be determined. A distribution function of something like $F(x) = x^{-1}$ would be ideal for a business, because then the majority of the exercise results are in the interval (a, b) between 1 and 0.5. This is the case represented by the curve Efk_I in Figure 8.

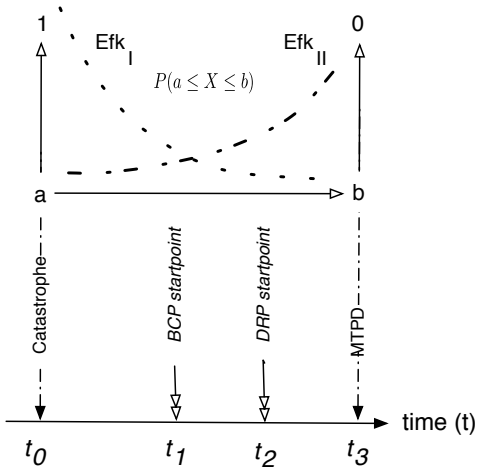

Fig. 8: Efk as a random variable within the interval a,b

In contrast, the curve Efk_{II} in Figure 8 represents an unfavorable curve for the indicator of effectiveness. In this case, the majority of the exercises are near the MTPD, i.e., near time t_3. Businesses that have displayed such an unfavorable course of effectiveness are not adequately equipped for a disaster and can probably survive only because of fortunate circumstances. This conclusion is in agreement with the empirical studies by Knight and Pretty [14].

Therefore, the closer a business's exercise results are to $x = 1$, the higher the probability that this business will survive a catastrophic event. However, these statements are valid only when plans such as BCP and DRP already exist when the disaster occurs and when these plans have been enacted, practiced, etc. Otherwise, measurements of indicators and key indicators–if no BCP or DRP is available–are meaningless. In that case, the cost curve is similar to curve 2 in Figure 5. Thus, an *ex-ante* statement would be possible only if sufficient information is available. Sufficient information is available if enough exercises in the BCP and DRP have been carried out.

The advantage to this method lies in the structured analysis of indicators and key indicators. This can also inform a board of management as to how a company is likely to respond to a disaster.

A. Key performance indicator of economic efficiency

The literature discussing cost considerations with regard to the security of information is controversial. A number of articles classify the calculation of the expenditure for security countermeasures in a Return of Security Investment (ROSI), often involving (perimeter) defensive techniques [23], [24], [25], [26]. A possible profit-loss of the organisation is confronted with the protection of IT assets and the costs of a successful attack are weighed against the security costs (countermeasures).

Other considerations in the literature deal with profit-loss as a loss of productivity; e.g., if a file server becomes unavailable, productivity declines because a number of employees become incapable of working [27]. Analysis of such problems are confounded because suitable material for a benchmark still does not exist [27].

Considerations of the profit-loss are aimed at increases in operating expenses and at influences on business processes. These impact economic efficiency. However, when considered in isolation, security costs represent only part of the economic efficiency of an BCMS.

Elsewhere it is argued that a cost consideration could not be successful with the ROSI model [28]. Further, it has been suggested that companies often apply a fear, uncertainty, and doubt (FUD) strategy for investments in security countermeasures [29]. A good overview of different approaches to the ROSI model is available in [25].

Note that the above approaches include neither indirect costs nor operating expenses in cost evaluations. In addition, direct costs are only partially taken into account. From the point of view of critical processes of an BCMS, the above approaches consider only partial aspects. With the efficiency of an BCMS, the focus is on the economic aspects of the BCPs and DRPs. For each rare risk that would have an huge impact on the value chain there must exist a BCP and DRP as well as all the processes and documents listed in Figure 7. Therefore, economic efficiency is to be thought of, in principle, as a cost/benefit relationship. To successfully plan the budget for the critical processes of an enterprise, the costs of all BCPs and DRPs must be considered.

A Total-Cost-of-Ownership (TCO) model provides an adequate look at the costs [30]. In the TCO model, three cost drivers are identified: direct costs (D_C), indirect costs (I_C), and operating expenses (O_C). At first glance, the TCO model seems to be sufficient for the interests of an BCMS when considering infrastructure costs. The three cost categories can be defined as follows:

- Sum of direct costs ($\sum_{i=1}^{n} D_{C_i}$): 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 costs of the devices (security appliances), their depreciation also has to be calculated.
- Sum of operating expenses ($\sum_{j=1}^{m} O_{C_j}$): Costs that must be considered when calculating the maintenance, servicing, and repair of the components listed as direct costs above.
- Sum of indirect costs ($\sum_{k=1}^{p} I_{C_k}$): 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 BCMS, that is, to the critical processes. In addition, the TCO model should not be of a static nature; instead, in the interest of increasing efficiency, it should be subject to a Deming cycle in accordance with ISO 9001.

As a modification, the TCO model, referencing a fiscal year, e.g., Fy_0 at t_0, could calculate the costs based on the infrastructure controls of the critical business processes of an BCMS. With this, the infrastructure costs of a BCMS in a fiscal year can be expressed as follows:

$$Fy_0 = \sum_{i=1}^{n} D_{C_i} + \sum_{j=1}^{m} I_{C_j} + \sum_{k=1}^{p} O_{C_k} \tag{19}$$

Then we can calculate a change (Iteration) from one fiscal year (Fy_0) at time t_0 to the next fiscal year (Fy_1) at time t_1. Besides the infrastructure costs, the expenses for the BCPs and DRPs need to be considered. An essential benefit of a BCMS is that it aims to establish a connection between cost and the recognized rare risks. In trying to define the economic efficiency of the risk defence with a BCP and DRP, a series of questions arise: According to Figure 7, the whole costs for all BCPs exercises (BCP_{costs}) and DRPs exercises (DRP_{costs}) for a BCMS can be derived from the pyramid carried out in one fiscal year, e.g. (Fy_0). This management is strictly carried out according to economic conditions. If, in the next fiscal year, a BCP/DRP exercise is again carried out at the time Fy_1, an optimization must have be done in between, because

- The processes for a BCP or a DRP can be optimized.
- The processes and controls, procedures, checklists can be optimized.
- The expenses for transferring the risks have changed (increased, decreased).
- In different (that is, in more then one) BCP and DRP the same controls, procedures, and checklists can be used.

As a result, a possible difference arises for the whole exercise cost of $\sum BCP_{costs}$ and for the whole exercise cost of $\sum DRP_{costs}$, which can be explained by a change in the cost of dealing with the BCP and DRP exercises and the increasing experiences. This means that the cost for a control that is used for one BCP/DRP could differ from that for a control that is used in more than one BCP/DRP.

So, for the KPI of the efficiency (Efz_k), which can be understood as the economic component with reference to an interval (Δt), when we consider the difference ($\Delta F \geq 0 = Fy_0 - Fy_1$) between the total BCP/DRP expenses for two fiscal years, we obtain

$$Efz_i = \frac{\left(\sum_{i=1}^{n} BCP_{iCost} + Fy_0\right) - \left(\sum_{i=1}^{n} BCP_{iCost'} + Fy_1\right)}{\sum_{i=1}^{n} BCP_{iCost} + Fy_0} \tag{20}$$

$$Efz_j = \frac{\left(\sum_{j=1}^{n} DRP_{j_{Cost}} + Fy_0\right) - \left(\sum_{j=1}^{n} DRP_{j_{Cost'}} + Fy_1\right)}{\sum_{j=1}^{n} DRP_{j_{Cost}} + Fy_0} \tag{21}$$

Equations 20 and 21 show that $Efz_{i,j} \in \mathbb{R}$ could be either a positive or a negative indicator. Nevertheless, in Eqs. 20 and 21, it is postulated that in the fiscal year Fy_1, a smaller budget is required for rare risk defence than in fiscal year Fy_0. Therefore, the key indicator is typically positive. Otherwise, if a larger budget is allocated than in the previous year, a negative indicator results.

The second key performance indicator (KPI_2) is related to the efficiency (Efz) of a BCMS. As mentioned above, a BCMS is a reactive model; in contrast, the ISO/IEC 27001 standard requires preventive controls related to the possible risks. Both a BCMS and an Information Security Management System (ISMS) according to ISO 27001 have risk management as a central component.

Bass and Robichaux discuss the different forms of handling preventive, detective, and corrective controls in connection with a baseline assurance [31]. If the ideas of [31] are applied, the question arises as to which of the recognized potential risks require preventive or reactive (corrective) actions. The present paper posits that this is merely a question of cost: it does not involve technical or organizational issues. Risk management corresponds to cost management and we know that a Business Continuity Management System (BCMS) according to BS25999 contains risk management. A similar result is found in [32].

In the case of a BCMS, this means that the reactive controls of each BCP and each DRP are cheaper to use than the value of business processes (value chain), and they are as cost effective as potential preventive (P_{rev}) controls. Thus, a cost inequality arises. Over a fiscal year ($Fy0$), the inequality involves these four costs: the cost of a each BCP (BCP_{cost}) and each DRP (DRP_{cost}), the additional costs (Adv_{cost}), and the cost ($P_{rev-Control_{cost}}$) for preventive controls,

$$Efz = BCP_{cost} + DRP_{cost} + Adv_{cost} \ll P_{rev-Control_{cost}} \ll Rev_{Fy0} \tag{22}$$

Here (Rev) is the business profit. The inequality (22) does not display static behavior. It provides a boundary condition for an ISMS in accordance with ISO 27001 and for a BCMS in accordance with BS 25999; however, the boundary conditions are temporal and must be periodically reviewed. It may well be that a potential risk can be dealt with more cheaply using a preventive action rather than a corrective/reactive one.

As an example, consider a company that is known to be located in a flood zone or an earthquake zone (see Figure 9). According to an ISMS, a preventive action would be to move the company. In contrast, a BCMS (BCP, DRP) would initiate action only after flooding or an earthquake occurred. The costs in light of the probability of risk must be balanced against each other, and this is precisely the inequality that is described by Eq. 22.

The indicators of effectiveness and economic efficiency have been determined in this section. In the next section, using the indicator of effectiveness, the performance will be determined.

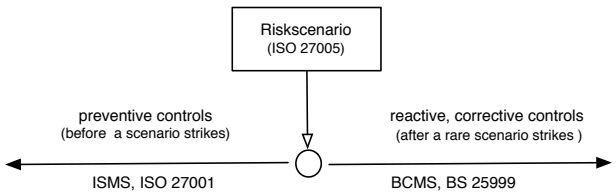

Fig. 9: Risk scenarios and the difference between ISMS and BCMS

B. Key performance matrix of effectiveness and efficiency

To determine the quality of a BCMS, the KPI of the effectiveness of a BCP must be placed in relation to the efficiency of a BCP. This takes into equal consideration both the efficiency (economic) and the effectiveness of a BCMS. These key indicators are two properties that should be kept strictly separated qualitatively and should not be aggregated into a single key indicator. The actual security countermeasures for critical business processes and their efficient realization can be shown in a matrix. Within the matrix, the KPIs of the effectiveness of the BCMS span one axis and the key indicators of efficiency span the other. The key performance indicators of effectiveness and of efficiency are bounded: $0 \leq Efk_k \leq 1$ and $-1 \leq Efz_k \leq 1$. The following can be defined as a first arbitrary linear approximation for effectiveness:

$$Efk_k = \begin{cases} yes & = & 0.5 < 1 \\ no & = & 0 \leq 0.5 \end{cases} \tag{23}$$

If the key indicator is above 0.5, the BCMS lies in the positive area (yes); if it is below 0.5, a (no) is assigned. A similar distinction can be defined for the key indicator of efficiency:

$$Efz_k = \begin{cases} yes & = & 0 < 1 \\ no & = & -1 \leq 0 \end{cases} \tag{24}$$

In principle all four possible combinations of Eq. 23 and Eq. 24 are observable; the four (a, b, c, d) are shown in Figure 10.

Case (a) can be described as an ideal state of a BCMS.

effective / efficient	yes	no
yes	a): BCMS is effective and efficient	b): BCMS is effective but not efficient
no	d): BCMS is not effective but efficient	c): BCMS is not effective nor efficient

Fig. 10: Performance matrix of an BCMS

a: *BCMS is effective and efficient*
This case can be defined as a strategic balance. Safeguarding critical business processes is in a strategic balance such that implementations of security controls are completely efficient. The BCMS supports the IT strategy efficiently with the right security controls, and the security controls are marked by an optimum cost/ benefit relationship.

In addition to the strategic balance, three kinds of imbalance exist for an IMS[4] [33]. Transferred onto a BCMS, the three correspond to the cases b, c, and d that appear in Figure 10.

b: *BCMS is effective but not efficient*
This situation corresponds to a strategic waste. The enterprise situation has high effectiveness due to the operation of an information security management system, but efficiency has not been achieved. In fact, in case (b), the achievement potential of an BCMS is effectively exhausted; however, exhaustion takes place uneconomically.

c: *BCMS is neither effective nor efficient*
This situation corresponds to a strategic dilemma. The operation of a BCMS and its achievement potential are neither effective nor efficient. Although considerable investments are expended in information security, the achievement potential is barely exhausted, and effective security countermeasures for critical business processes are not realized. Dissipation and waste of valuable resources exist.

d: *BCMS is not effective, but it is efficient*
This situation corresponds to a strategical dissipation. The efficiency of the BCMS is high, but its effectiveness is very low. The achievement potential of the BCMS is not properly recognised nor exhausted. Every control in information security is considered unique and, hence, is often misjudged.

If a performance $(Efk_k; Efz_k)$ measurement finds any imbalance (b, c, d), the BMCS must act as in Figure 11. The actuator initiates the check-and-act phases of the PDCA cycle so that corrective and preventive actions are performed. This process should continue until a balance between effectiveness and efficiency is attained, i.e., until case (a) is realized. Figure 11 shows this operation within a control loop according to a deterministic finite state machine.

Moreover, even if a company is already in the range of the strategic balance, further improvements may be possible, leading to minimal turnover. This improvement can be obtained via a combinatorial optimization between the KPI of effectiveness and the KPI of efficiency for each BCP. We present this idea in detail in the next section.

VI. Trade-off between effectiveness and efficiency

To perform a cost benefit analysis of information security, this article proposes two KPIs. For each KPI, suitable measurable indications are defined. The KPI of effectiveness and

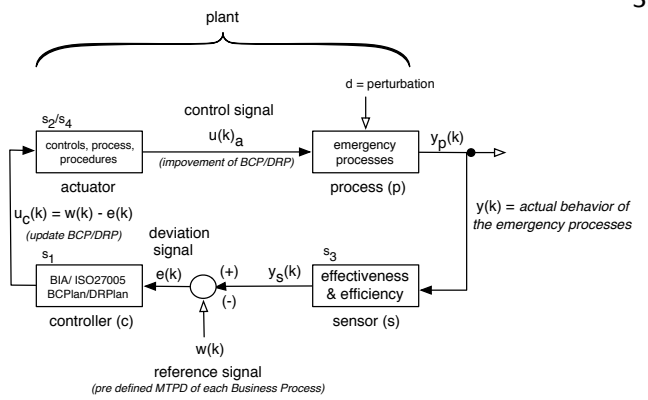

Fig. 11: Control loop for a BCP

the KPI of economic efficiency compete (Fig. 12), so that an alignment in favor of one KPI is necessarily done at the expense of the other. In [13], a key performance matrix with four ranges is presented according to the ISMS and in [34] a similar trade-off approach is presented for an ISMS.

The best range of values for the KPIs is the strategic balance in which the KPI of effectiveness and the KPI of efficiency support the economic strategy and achieve a suitable cost/benefit relationship. One of the main task of an BCMS with its PDCA-Cycle is to reach the strategic balance.

To optimize the BCP/DRP, requirements must be positioned so as to maximize effectiveness in the direction of a strategic balance. This means, for instance, that more exercises must be done for all working instructions, records, and policies structured according to Figure 7 procedures (objective evidence of policy enforcement). This would reduce the risk that the BCP/DRP was not working very well. However, this requirement would exceed the calculated budget. With regards to economic efficiency, one attempts to minimize the cost for each BCP/DRP with respect to investments so as to reduce turnover as little as possible.

Figure 12 shows the two KPIs like contrasting faces. The graphs are based on typical behaviour and we present a first approximation. The introduced budget limit of 30% is taken from the Ph.D. thesis from Soo Hoo on an empirically determined limit of investment [35]. This trade-off can be interpreted as a variation of the knapsack problem (KP). The knapsack problem is an integer combinatorial optimization problem and is $\mathcal{NP}-hard$. This means that a ROSI calculation has a complex solution.

This description of the 0-1 knapsack problem follows Martello[5] and Toth [36]. To use the approach from Martello and Toth for this trade-off, it is necessary to determine an optimum for the cost of each BCP/DRP with some certain controls (x) related to some certain policies (p) within the limited predefined investment [35]. In this 0-1 knapsack approach, we use for the controls $x_j(j = 1, ...n), n \in \mathbb{N}$, which could reduce one or more risks from the SoA through countermeasures

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

[5]cf. Martello & Toth, page 1–5

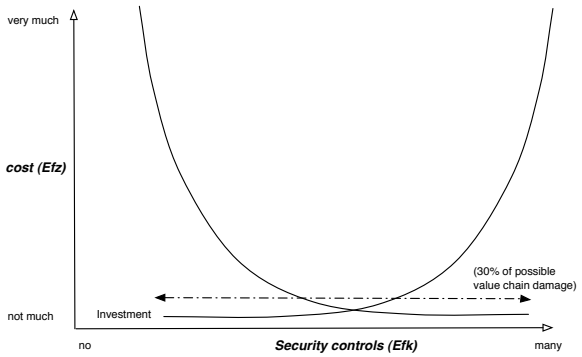

Fig. 12: Trade-off between Efz_k and Efk_k

(controls, x_j),

$$x_j = \begin{cases} 1 & = \text{ if control j is being used;} \\ 0 & = \text{ otherwise} \end{cases} \quad (25)$$

Furthermore, we use p_j for policies (P_{ol}) and w_j for the cost of each control x_j. Hence, a policy that is able to reduce more than one risk is more welcome; otherwise, it is better to mitigate a risk than to avoid it. Like Soo Hoo, we use c to describe the upper investment limit.

The definitions are as follows:

p_j: policy in terms of benefit from each control x_j,
w_j: cost for each control, which considers each BCP/DRP,
c: upper investment limit from Soo Hoo.

We expect that policies reduce more than one risk, in accordance with Eq. 19, so we try to optimize the function z,

$$maximize\ z = \sum_{j=1}^{n} = p_j x_j \quad (26)$$

We interpret p_j as a policy to confront risk; therefore, the value p_j for safeguarding the critical business process (cBP) will increase when p_j mitigates more than one risk under the side condition of w_j. Now, we attempt to figure out for which controls in (x) the following is valid:

$$\sum_{j=1}^{n} = w_j x_j \leq c \quad (27)$$

With Eqs. (25), (26), and (27), we can define a 0-1 knapsack problem. To solve the complexity of this 0-1 knapsack problem, this paper proposes a heuristic procedure. In Martello and Toth [36], different heuristic solution are discussed. In our contribution, the Branch-and-Bound (BB) procedure of the Horowitz-Sahni algorithm (HS) was chosen as a first approximation. The Branch and Bound procedures are essentially based on a problem branching and a limitation by means of lower and upper bounds for the subsets.

1) Branch: The basic principle of the Branch and Bound procedure is based on a minimization. A forward movement consists of inserting the largest possible set of new consecutive items into the current solution. A branching of the problem (P_0) is performed, yielding $k = 3$ subproblems $P_i\{1 = 1...k\}$, so that the following is an allowable solution for the subset (x_j):

$$x(P_0) = \bigcup_{i=1}^{k} x(P_j) \quad (28)$$

The three sub-problems can be thought of as the controls that are used in more than one BCP/DRP. The following subproblems then exist: $P_1(BCP_a)$, $P_2(BCP_b)$, $P_3(BCP_c)$.

2) Bound: Still, for each subset there are limitations, namely a lower bound (LB) and an upper bound (UB). If it is valid that $LB \geq UB$ is a set of a solution, this set will not be investigated further (elimination of uninteresting subsets). The ideal value of the upper boundary for P_0, like an optimal approximation, must be found heuristically. As a first approximation, Soo Hoo's budget limit of 30% can be used. During the process, the UB corresponding to the current solution of P_0 is computed and compared with the current best solution. If $LB_i < UB$ and if the optimal solution is $P_1^{'}$ and is valid for P_i or P_0, then a new best solution has been found for P_0 and we replace $UB := LB_i$.

Finally, an example of a Horowitz-Sahni algorithm is shown in Figure 13. This algorithm has been used with the Fortran program from the book [36]; an example is calculated with the following data. The simple example is given by solving the Horowitz-Sahni algorithm for a given set of policies (P_{ol}) which is a special Indicator on the first level ($I_{\lambda_1} = 7$), a simple given set of $n = 7$ controls (x_j, $j = 1, ...7$), a current solution $\hat{z}$, and a current best solution z. For a given set of policies, we can elaborate on

p= $\{70, 20, 39, 37, 7, 5, 10\}$ which are useful for more than one BCP. The scale is 1,...,100 units. To face each BCP/DRP and control (consult Eq. 28) for a given set of cost of controls, also in a scale of 1,...,100 units, we use
w= $\{31, 10, 20, 19, 4, 3, 6\}$.
c= $\{50\}$ is the size of the capacity of knapsack we use.

We present the results in Figure 13. In this example, u is an upper bound and $\hat{x}_j$ is a current solution. The best solution so far is x_j.

Finally we can draw a short result from this trade-off analysis. If a company is in the range of the strategic balance between the effectiveness and the efficiency of its BCMS according to BS25999 and, if the company needs to have further improvement to reduce turnover to as little as possible, then a combinatorial optimization is very useful. Such an optimization should balance the benefit of a policy in terms of risk, which is considered for each control, and the cost of each control in terms of avoiding, mitigating, or transferring the risk to a determined limit of investment.

VII. Conclusion and future work

The empirical studies by Knight and Pretty [14] suggest that the quality of a BCMS, as well as the related BCP and DRP, should be looked at more intensely: the existence of a BCMS in accordance with BS 25999 does not necessarily say

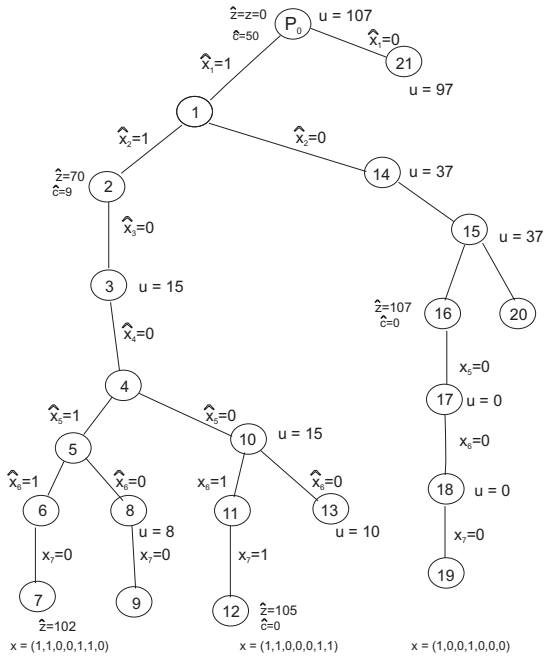

Fig. 13: Example with Horowitz-Sahni Algorithm

anything about survival probability in the event of a disaster. Survival depends on the implementation of the BCMS, and here the BCP and DRP are interpreted as reactive controls of great importance to survival in the event of a disaster.

In this paper the importance of the output and efficiency of a BCP and DRP have been demonstrated using indicators. Furthermore, it has been shown that by using two indicators, the effectiveness and economic efficiency of a BCMS can be measured. These two indicators represent key performance indicators for a company. If there are a number of measurements for effectiveness, a forecast can be made based on a random variable in terms of survival probability, but this can be done only if there is sufficient experience in applying the BCP and DRP. In addition, these key performance indicators can be used by a company to document its performance.

However, this method of using indicators evaluates the processes behind the BCP and DRP only approximately. The disadvantage of the method is that there must be sufficient experience in using the BCP and DRP; therefore, a company is not well prepared for catastrophes that are unknown. Combinations of or additions to the BCP and DRP based on similar catastrophic scenarios are only possible if the processes behind the BCP and DRP are exercised in advance using relevant types of simulations.

Unfortunately, there are still no appropriate methods to pursue these ideas. Currently, processes are typically associated with the layout of an event-driven Process Chain (ePC), which is merely a snapshot of processes, not a simulation in the sense of running a complete process. These considerations may suggest approaches for further investigation.

References

[1] W. Boehmer, "Survivability and Business Continuity Management System According to BS 25999," *Proceedings of the Emerging Security Information, Systems and Technologie, 2009. SECUWARE '09, Third International Conference on, IEEE Computer Society*, pp. 142–147, June, 18-23 2009.

[2] BS25999-1, "Business Continuity Management System – Part 1: Code of practice, BSI (UK)." ISBN 0580496015, 11 2006.

[3] BS25999-2, "Business Continity Management System – Part 2: Specification, BSI (UK)." ISBN 9780580599132, 11 2007.

[4] IBM, "Panic slowley. integrated disaster response and bulit-in business continuity," ibm.com/itsolutions/uk/governance/businesscontinuity, 2006.

[5] SC27, "ISO/IEC 27001:2005, Information technology - Security techniques - information security management systems - Requirements." Beuth-Verlag, Berlin, 10 2005.

[6] ITGI, "Cobit, control objective in information and related technology, 4th. ed.." IT Governance Institute, ISBN 1-933284-37-4, 2006.

[7] C. Brandt, T. Engel, W. Boehmer, and C. Roeltgen, "Diskussionsvorschlag einer Lösungsskizze zur Behandlung von operationellen IT-Sicherheitsrisken nach Basel II auf der Grundlage von Anforderungen der Credit Suisse," in *Multikonferenz Wirtschaftsinformatik, München, MKWI2008*, 2008.

[8] W. Boehmer, C. Brandt, and J. F. Groote, "Evaluation of a business continuity plan using process algebra and modal logic," in *2009 IEEE Toronto International Conference – Science and Technology for Humanity TIC-STH 2009 - SIASP 2*, pp. pp. 147–152, Ryerson University, 245 Church Street, Toronto, Ontario, Canada, 2009.

[9] W. Boehmer, C. Brandt, and J. Groote, "Evaluation of a business continutiy plan using process algebra and modal logic," *Computer Science Report CSR-09-12, Eindhoven University of Technology,*, 2009.

[10] M. Alemanni, G. Alessia, S. Tornincasa, and E. Vezzetti, "Key performance indicators for PLM benefits evaluation: The Alcatel Alenia Space case study," *Comput. Ind.*, vol. 59, no. 8, pp. 833–841, 2008.

[11] R. R. Rodriguez, J. J. A. Saiza, and A. O. Basa, "Quantitative relationships between key performance indicators for supporting decision-making processes," *Computer in Industry*, 2008.

[12] L. Tsinas, B. Trösken, and S. Sowa, "KPI-Framework für Informationssicherheit," 2009.

[13] W. Boehmer, "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," *Emerging Security Information, Systems, and Technologies, The International Conference on (SECUWARE 2008), IEEE Computer Society*, vol. 0, pp. 224–231, 2008.

[14] K. R. and P. D., "The impact of catastrophes on shareholder value," the oxford executive research briefings, Templeton College, University of Oxford, Oxford, England, 1996.

[15] M. Nemzow, "Business continuity planning," *Int. J. Netw. Manag.*, vol. 7, no. 3, pp. 127–136, 1997.

[16] G. Quirchmayr, "Survivability and business continuity management," in *ACSW Frontiers '04*, (Darlinghurst, Australia), pp. 3–6, Australian Computer Society, Inc., 2004.

[17] B. J. L. Landry and M. S. Koger, "Dispelling 10 common disaster recovery myths: Lessons learned from Hurricane Katrina and other disasters," *J. Educ. Resour. Comput.*, vol. 6, no. 4, p. 6, 2006.

[18] K. Saleem, S. Luis, Y. Deng, S.-C. Chen, V. Hristidis, and T. Li, "Towards a business continuity information network for rapid disaster recovery," in *dg.o '08: Proceedings of the 2008 international conference on Digital government research*, pp. 107–116, Digital Government Society of North America, 2008.

[19] I. Shklovski, L. Palen, and J. Sutton, "Finding community through information and communication technology in disaster response," in *CSCW '08: Proceedings of the ACM 2008 conference on Computer supported cooperative work*, (New York, NY, USA), pp. 127–136, ACM, 2008.

[20] S. Tjoa, S. Jakoubi, and G. Quirchmayr, "Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology," in *ARES '08,*, (Washington, DC, USA), pp. 179–186, IEEE Computer Society, 2008.

[21] J. Lunze, *Ereignisdiskrete Systeme; Modellierung und Analyse dynamischer Systeme mit Automaten, Markovketten und Petrinetzen*. ISBN 3-486-58071-X, Oldenbourg Verlag, 1. auflage ed., 2006.

[22] A. Calder, "PDCA Cycle & Documentation Pyramid." IT Governance: a Manager's Guide to Data Security and ISO27001/27002, ISMS Toolkit, 2007.

[23] J. Eloff and M. Eloff, "Information Security Architecture," *Computer Fraud & Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[24] D. Larochelle and N. Rosasco, "Towards a Model of the Costs of Security," *Technical Report CS-2003-13, University of Virginia, Dept. of Computer Science.*, 06 2003.

[25] T. Tsiakis and G. Stephanides, "The economic approach of information security," *Computers & Security*, vol. 24, pp. 105 –108, March 2005.

[26] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[27] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI) - A Practical Quantitative Model," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. p. 45–56, 2008.

[28] *Return on security investment – proving its worth it*, vol. 2005, 2005.

[29] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments," *Commun. ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[30] J. S. David, D. Schuff, and R. S. Louis, "Managing your total IT cost of ownership," *Commun. ACM*, vol. 45, no. 1, pp. 101–106, 2002.

[31] T. Bass and R. Robichaux, "Defense-in-depth revisited: Qualitative risk analysis methodology for complex networkcentric operations," *IEEE MILCOM*, vol. 2001, pp. 28–31, 2001.

[32] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, (New York, NY, USA), pp. 97–104, ACM, 2001.

[33] L. Heinrich and F. Lehner, *Informationmanagement, Planung, Überwachung und Steuerung der Informationsinfrastruktur*. ISBN-13:9783486577723, Oldenbourg Verlag, 8. auflage, seite 84, ff ed., München, 2005.

[34] W. Boehmer, "Cost-benefit trade-off analysis of an ISMS based on ISO 27001," *ARES Conference, The International Dependability Conference, IEEE Computer Society*, pp. 392 –399, March, 16th. – 19th. 2009.

[35] K. S. Hoo, *How Much is Enough? A Risk Management Approach to Computer Security;*. PhD thesis, Stanford University, CRISP, 2000.

[36] S. Martello and P. Toth, *Knapsack Problems, Algorithms and Computer Implementations*. ISBN 0471924201, John Wiley and Sons Ltd., 1990.