Survivability and Business Continuity Management System According to BS 25999

Wolfgang Boehmer*
*University of Technology Darmstadt, Germany, Hochschulstr. 10, 64289 Darmstadt
Email: wboehmer@sec.informatik.tu-darmstadt.de

***Abstract*—In this paper, a new model is presented for evaluating the performance of a Business Continuity Management System according to BS 25999. This model is able to calculate the survivability *ex-ante* if the key performance indicator for the effectiveness exists. Performance is based fundamentally on the system's Business Continuity Plans and Disaster Recovery Plans. Typically, the performance of these plans is evaluated by a number of specific exercises at various intervals and, in many cases, with a variety of targets. Furthermore, these specific exercises are rerun after a longer period (≥ a year) and then often only partially. If a company is interested in taking performance measurements over a shorter period, obstacles and financial restrictions are often encountered. Furthermore, it is difficult for companies to give an *ex-ante* statement 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.**

***Index Terms*—BS 25999; BCMS; Business Continuity Plan (BCP); Disaster Recovery (DR).**

I. Introduction

The BS 25999-1:2006 standard sets out the code of practice for a Business Continuity Management System (BCMS) [16]. After extensive review by the British Standard Institution (BSI), BS 25999-2:2007, on the specifications for Business Continuity Management (BCM), was published in November 2007 [17]. During this review, more than 5000 industrial ideas and suggestions were integrated into the standard, thus setting out a high degree of maturity. The scope of the standard BS 25999-2:2007 provides requirements for a management system for the stability of critical business processes (value chain) to an acceptable level for disasters. The fundamental idea of a BCMS is based on the fact that BCM aims to manage various types of uncommon business risks that 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.

The BS 25999 standard requires the implementation of a management system in accordance with the PDCA cycle (Plan–Do–Check–Act) as well as those systems already required in, among other standards, ISO 27001 and ISO 20000. The PDCA cycle is based on the idea of imperfection and thus follows a continuous improvement process. In the Check phase, e.g., it is examined whether the plan with the objective set is still in agreement with the rest of the system. If not, the corrections are resolved in the Act stage. The initial Plan

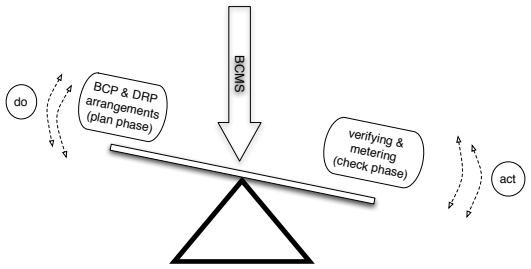

Fig. 1: Business Continuity Management System (BCMS) represented as a seesaw

phase of the PDCA cycle in the management system of BS 25999 requires the identification of critical business processes and an 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 BCP must be developed as a response. The response is aimed, on the one hand, at continuing the effect of the business processes on a defined level (BCPs) and, on the other, at initiating the corresponding countermeasures that will restore the original state (Disaster Recovery Plan; DRP).

As in the ISO 27001 standard, risk also plays a central role in BS 25999 [15][17]. However, while the measures for the implementation of ISO 27001 are risk-prevention oriented, those for BS 25999 (BCP and DRP) are reactive (see Figure 3). BCM is a reactive model that becomes active only after the disaster has occurred. In this context, the maximum allowable downtime (Maximum Tolerable Period of Disruption; MTPD), which starts running after the disaster occurs, increases considerably in importance. The MTPD is determined using the length of time the critical activities of the value chain require to begin working again after a disaster in order for the company to survive (see Figure 4). This period of time ($\Delta T_{max} = t_0 \rightarrow t_3$) is an ultimate boundary for a company and decides the company's survival. If this ultimate limit is exceeded, the company is irretrievably lost (see curve (2), Figure 4). 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 the critical activities (core processes of the value chain) are analyzed. Any BCMS includes those business processes that are vital. A reduced scope of the IT systems will not meet a BCMS, as clearly pointed out in an IBM report [5].

The goal of every company must therefore be to optimize the performance of the restoration and the time required for this restoration (Recovery Time of Objective; RTO). Thus, a company must do everything to ensure that RTO ≤ MTPD can be achieved. However, the efficiency of the restoration measures must not be ignored.

In the literature, two basic methods are generally described for measuring performance.

- On the one hand, performance can be measured on the maturity of processes, such as with Spice (ISO/IEC 15504) or CMMI.
- On the other hand, performance can be measured on the basis of appropriate indicators (key performance indicators; KPI). Proposals for the handling of key indicators can be found in the literature, e.g., [1][11].

In this article, performance indicators for effectiveness and economic efficiency are measured. However, performance, as in CobiT, is also understood here [6]. A measurement will take place in the Check phase as mentioned above. However, the standard describes only *what* to do rather than *how* to do it.

In a previous article by Boehmer, it was demonstrated how the management system of ISO 27001 can be measured by the indicators of effectiveness and efficiency [3]. This idea of measuring the quality of these two KPIs is applied to a BCMS in the present paper. Measurements of these KPIs provide the status of a BCMS and one of four quadrants mapped. The worst state is one in which a BCMS is neither effective nor efficient, and is called a strategic dilemma [3]. Consequently – in the case of a strategic dilemma – the probability of the occurrence of a catastrophe 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 four sections. The following section focuses on integrating work from the relevant literature. Then, in the third section, the structure of a process-oriented evaluation system based on circumstantial evidence and key indicators will be discussed. In the fourth section, the development of two KPIs is discussed, then used in the fifth section to look at survival probability. Survival probability is closely linked to a functioning BCP. The article concludes with an outlook and a brief summary.

II. Related Work

One empirical study by Knight and Pretty shows that those companies with a BCMS are more likely to survive a disaster than those who have taken no precautions [10]. 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 cases in which no BCMS was used in companies that still survived a disaster [10]. This latter phenomenon may simply be down to luck.

Looking at those cases of companies that used a BCMS and still did not survive, it appears the quality of the BCMS or BCP and DRP used needs to be taken into account. It is clear from the study that the application of a standard alone is not enough, since, apparently, this was inadequately applied in these cases.

The literature has so far focused on the topic of BCMS primarily in practical terms, e.g., [8][9][7]. In [8] Nemzow discusses the need for various strategies toward natural and manmade disasters in order to protect an organization. Nemzow also explains the difference between a BCP and DRP. Quirchmayr discusses in [9] the Business Continuity Management Lifecycle and its content. Landry and Koger discuss the lessons learned from 2005's hurricane Katrina [7]. Again, the importance of a DRP is stressed. A similar set of ideas is set out in the study by IBM on hurricane Katrina and claims that a BCP and DRP include more than simply aspects of the company. Company members left behind in the disaster area should also be taken into account in the BCP [5]. Similarly, Saleem et al. [12] note the importance of an adequate Business Continuity Information Network on an effective DRP. A similar issue is also highlighted by Shklovski et al. [13]. The importance of Business Impact Analysis (BIA) and the restoration point of objective after a disaster is discussed by Quirchmayr et al. [14]. 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 [10]. 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 the performance has been measured can a statement be made on a business's survival probability.

III. Performance Indicator of a BCMS according to BS 25999

This section shows how the key indicators of effectiveness and economic efficiency are developed. A number of indicators will be formed for each key indicator. A definition exists for an indicator and one for a key indicator:

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. 10 and Eq. 11).

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, DRP in the Check phase (see Figure 1). For the system's effectiveness, this means that the indicators

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

form a set of the system effectiveness (Efk):

$$Efk = \{I_{ex}, I_{op_{(BCP,DRP)}}, I_{co}\}. \tag{1}$$

These indicators are derived from pyramid-level documents (see Figure 2). This pyramid structure was derived by Alan Calder from practical experience and published in the ISMS Toolkit [4].

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.

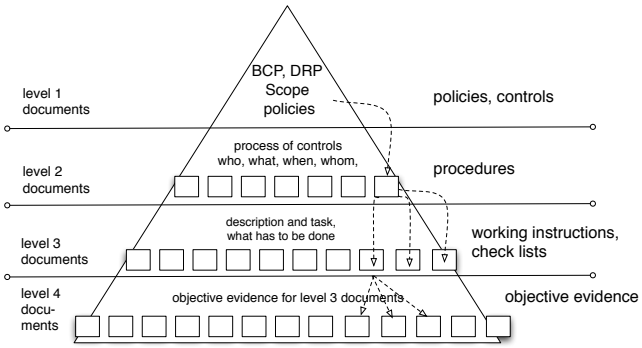

Fig. 2: Pyramid-level documents of a BCP and DRP

Figure 2 shows how the volume of documents from the top (peak) down increase. This structure shows the natural history based on a directive toward their technical implementation (procedures, checklists), which provides a series of activities for implementing the directive. At the lowest level is the evidence *(objective evidence*), as described by Alan Calder [4]. This pyramid structure is now a condition for the existence of a lower boundary, as recommended in [3]. 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.

A. Key performance indicator of system effectiveness

The first key performance indicator (KPI_1) relates to the effectiveness (see Eq. 1), 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 on the implementation of the standards. This case of the existence or non-existence of control points per level can be shown as:

$$I_{ex} = \frac{\sum_{i=1}^{n} CP_{\lambda i} - \sum_{j=1}^{m} NoCP_{j(BCMS)}}{\sum_{i=1}^{n} CP_{\lambda i}} \tag{2}$$

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

$$I_{ex} = \begin{cases} 1, & falls\ NoCP = 0 \\ 0, & falls\ \forall\ CP_{\lambda i} = 0 \\ otherwise, & \end{cases} \tag{3}$$

For the ideal implementation of each standard in a business, the goal is for the indicator to be within a range of $I_{ex} \approx 1$ for each standard. This would mean that there are no deviations ($NoCP \approx 0$) between the control points (clauses) of the standards with the actual existing control points. In the case of $I_{ex} \ll 1$, this means that 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. 3 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 ($C_{\lambda i(BCP)}$) relative to the pyramid-level documents. Whether adequate controls for a particular risk scenario (see Figure 3) 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, for example, a scenario for the risk that a major supplier *(key stakeholder)* fails unexpectedly.

The indicator of the degree of enforcement ($I_{op_{(BCP)}}$) checks (Eq. 4) the extent of discrepancies in the assessments between the action in BCP ($C_{\lambda i(BCP)}$) and the actual sequence ($NoC_{j(BCP)}$) in an exercise.

$$I_{op_{(BCP)}} = \frac{\sum_{i=1}^{n} C_{\lambda i(BCP)} - \sum_{j=1}^{m} NoC_{j(BCP)}}{\sum_{i=1}^{n} C_{\lambda i(BCP)}} \tag{4}$$

Thus, the indicator of the control points $I_{op_{(BCP)}}$ is in the range between 0 and 1 and is analogous to Eq. 3.

$$I_{op_{(BCP)}} = \begin{cases} 1, & falls\ NoC_{(BCP)} = 0 \\ 0, & falls\ \forall\ C_{\lambda i(BCP)} = 0 \\ otherwise, \end{cases} \tag{5}$$

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 ($C_{\lambda i(DRP)}$) controls.

$$I_{op_{(DRP)}} = \frac{\sum_{i=1}^{n} C_{\lambda i(DRP)} - \sum_{j=1}^{m} NoC_{j(DRP)}}{\sum_{i=1}^{n} C_{\lambda i(DRP)}} \tag{6}$$

Thus, the indicator of the control points $I_{op_{(DRP)}}$ is in the range between 0 and 1 and is analogous to Eq. 3. This indicator assesses the difference between the planned activities and the actual exercises.

$$I_{op_{(DRP)}} = \begin{cases} 1, & falls\ NoC_{(DRP)} = 0 \\ 0, & falls\ \forall\ C_{\lambda i(DRP)} = 0 \\ otherwise, \end{cases} \tag{7}$$

Equation 7 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 the coverage. The indicator (I_{co}) of the coverage of a BIA in relation to resources (key products, stakeholders, etc) within the scope leads to:

$$I_{co} = \frac{\sum_{i=1}^{n} Res_{i(BIA)} - \sum_{j=1}^{m} Res_{j(NoSP)}}{\sum_{i=1}^{n} Res_{i(BIA)}} \tag{8}$$

Equation 8 places the critical resources (Res) within the BIA that must be treated with non-existing policies ($NoSP$) in relation to resources.

$$I_{co} = \begin{cases} 1, & falls\ Res_{(NoSP)} = 0 \\ 0, & falls\ \forall\ Res_{(BIA)} = 0 \\ otherwise, \end{cases} \tag{9}$$

Thus, the indicator (I_{co}) is in the range between 0 and 1 and is analogous to Eq. 3. 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 the effectiveness can be calculated with:

$$Efk = I_{ex} \times I_{op_{(BCP)}} \times I_{op_{(DRP)}} \times I_{co} \tag{10}$$

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 4), a conclusion may be drawn about the likelihood of survival in the event of a disaster. This aspect is detailed in Section IV.

B. Key performance indicator of economic efficiency

The second key performance indicator (KPI_2) relates to the efficiency (Efz) of a BCMS. As mentioned above, a BCMS is a reactive model, while the ISO/IEC 27001 requires preventive controls related to the possible risks. In an article by Bass and Robichaux, they discuss the different forms of handling preventive, detective and corrective controls in connection with a baseline assurance [2]. Both a BCMS as well as an Information Security Management System (ISMS) according to ISO 27001 have risk management as a central component. If the ideas of [2] are applied, so the question arises as to which of the recognized potential risks are evidenced with preventive or reactive (corrective) actions. The present paper posits that this is merely a question of cost and does not involve technical or organizational issues.

In the case of a BCMS, on the one hand, this means that the reactive controls of a BCP and DRP are cheaper to use than the values of business processes (value chain) and are as cost effective as the potential preventive (P_{rev}) controls. Thus, a cost inequality arises. The cost of a BCP (BCP_{cost}) and DRP (DRP_{cost}) and the additional costs (Adv_{cost}) and cost ($P_{rev-Control_{cost}}$) for the preventive controls, together with the business profit (Rev), are set in relation to a fiscal year ($Fy0$).

$$Efz = BCP_{cost} + DRP_{cost} + Adv_{cost} \ll P_{rev-Control_{cost}} \ll Rev_{Fy0} \tag{11}$$

This inequality (Eq. 11) 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; conversely, the boundary conditions are temporal and must be periodically reviewed. It may well be that a cheaper identified potential risk can be dealt with as a preventive rather than a corrective/reactive action.

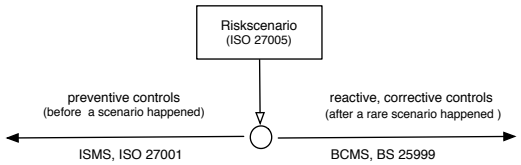

Fig. 3: Risk scenarios and the difference between ISMS and BCMS

As an example of a risk scenario (see Figure 3), we can take a company that is known to be, for example, located in a flood zone or an earthquake zone. According to an ISMS, a preventive action would be to move the company. A BCMS (BCP, DRP) would initiate action only after the occurrence

of flooding or an earthquake. The costs in the light of the probability of risk must be balanced against each other. This is precisely the inequality as described in Eq. 11.

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

IV. 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 (Eq. 1) and economic efficiency (Eq. 11) have been identified.

When economic efficiency is considered in advance (preventive or reactive controls) of a balance of controls, this indicator is not used for the consideration of the likelihood of survival.

Figure 4 shows qualitatively, on a money/timeline, the processes after a disaster occurs at time t_0 for a business. This shows that, immediately after the occurrence of a disaster, the calculated turnover collapses. At time t_1 the processes of the BCP (emergency operation) start and result in a turnover at an acceptable level. A little later, at time t_2, the processes of recovery run to the end of normal condition when time t_4 is reached. The dash-dotted line in the figure shows that the cost increases after a disaster. In the event that no controls (BCP, DRP) are taken, or that the controls do not work, the cost continues to increase (see curve (2)). If they exist to a sufficient extent, BCP and DRP then influence the cost, as shown by curve (1).

If no action (BCP, DRP) has been taken at time t_3 or has not been started until time t_3, then the cost will increase until company insolvency is reached (see Figure 4). The costs are determined by the obligations of the company. These are primarily personnel costs, technical expenses and the costs of delivery, performance, and possibly storage costs, etc.

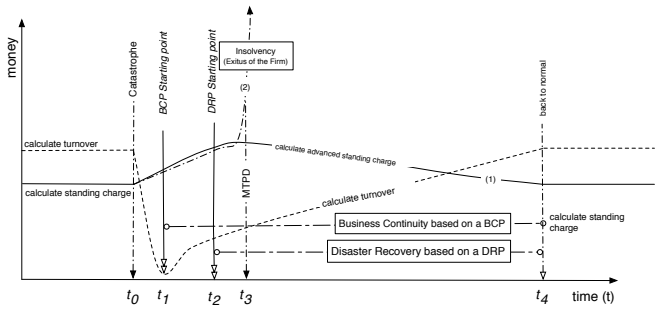

Fig. 4: Illustration of the aspects of a catastrophe (t_0) and the reaction ($t_1, ..., t_4$)

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 5). Figure 5 shows only the part between t_0, t_3 (cf. Figure 4). Here, *(a)* can be defined as the entry point at a time of disaster and *(b)* as the date defined by the MTPD. Figure 5 marks the interval *(a,b)* with the 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 ($x =$) in the ideal case, this means that (t_0) and (t_1) almost coincide and the starting point of the BCP is immediately after the occurrence of the disaster. Vice versa is also true: the smaller that ($x \ll$) is, the later that time (t_1) is, 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 und 0.5. This case illustrates some of the quality curve, with Efk_I characterized.

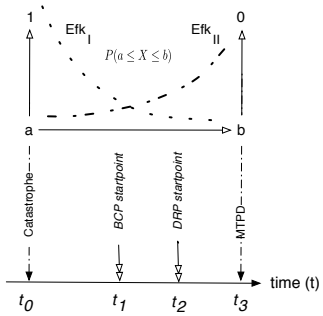

Fig. 5: Efk as a random variable within the interval a,b

The second case shows an example of an unfavorable curve of the indicator of effectiveness. The curve characterized by Efk_{II} shows a case in which the majority of the exercises are near MTPD, i.e., at 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 therefore in agreement with the empirical studies by Knight and Pretty [10].

The closer a business's exercise results are to $x = 1$, the higher the probability that this business will survive a catastrophic event.

However, it must be noted that these statements are valid only when such plans (BCP, DRP) already exist when the disaster occurs and when these plans have been enacted, practiced, etc. Otherwise, the measurement of indicators and key indicators – if no BCP or DRP is available – is meaningless. In that case, the curve of cost is similar to curve (2) in Figure 4. 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 of this method lies in the structured analysis of indicators and key indicators. This can also form guidance for a board of management as to how the company is likely to respond in the event of a disaster.

V. Conclusion and future work

The empirical studies by Knight and Pretty [10] suggest that the quality of a BCMS should be looked at more intensely, and the related BCP and DRP, because the existence of a BCMS in accordance with BS 25999 does not necessarily say something about the survival probability of a company in the event of a disaster. It depends on the implementation of the BCMS. Here, the BCP and DRP are reactive controls of great importance for the survival probability in the event of a disaster. This importance of the output and efficiency of a BCP and DRP has been shown in this paper 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 only if there is sufficient experience in the application of the BCP and DRP. Furthermore, a company can document its performance through these key performance indicators.

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 for the BCP and DRP, and therefore, a company is not well prepared for catastrophes that are unknown. A combination of or an addition to the BCP and DRP based on similar catastrophe scenarios is not possible. This would be possible only if the processes behind the BCP and DRP are put through the relevant type of simulation in advance. However, there are still no appropriate methods to pursue these ideas. Currently, the processes are typically associated with the layout of the event-driven Process Chain (ePC), which is merely a snapshot of processes but not a simulation in the form of running a complete process. These considerations may form approaches for further investigation.

References

[1] Marco Alemanni, Grimaldi Alessia, Stefano Tornincasa, and Enrico Vezzetti. Key performance indicators for plm benefits evaluation: The alcatel alenia space case study. *Comput. Ind.*, 59(8):833–841, 2008.

[2] Tim Bass and Roger Robichaux. Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. *IEEE MILCOM*, 2001:28–31, 2001.

[3] 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*, 0:224–231, 2008.

[4] Alan Calder. Pdca cycle & documentation pyramid. IT Governance: a Manager's Guide to Data Security and ISO27001/27002, ISMS Toolkit, 2007.

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

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

[7] Brett J. L. Landry and M. Scott Koger. Dispelling 10 common disaster recovery myths: Lessons learned from hurricane katrina and other disasters. *J. Educ. Resour. Comput.*, 6(4):6, 2006.

[8] Martin Nemzow. Business continuity planning. *Int. J. Netw. Manag.*, 7(3):127–136, 1997.

[9] Gerald Quirchmayr. Survivability and business continuity management. In *ACSW Frontiers '04: Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation*, pages 3–6, Darlinghurst, Australia, Australia, 2004. Australian Computer Society, Inc.

[10] Knight R. and Pretty D. The impact of catastrophes on shareholder value. The oxford executive research briefings, Templeton College, University of Oxford, Oxford, England, 1996.

[11] Raul Rodriguez Rodriguez, Juan José Alfaro Saiza, and Angel Ortiz Basa. Quantitative relationships between key performance indicators for supporting decision-making processes. *Computer in Industry*, 2008.

[12] Khalid Saleem, Steven Luis, Yi Deng, Shu-Ching Chen, Vagelis Hristidis, and Tao 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*, pages 107–116. Digital Government Society of North America, 2008.

[13] Irina Shklovski, Leysia Palen, and Jeannette 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*, pages 127–136, New York, NY, USA, 2008. ACM.

[14] Simon Tjoa, Stefan Jakoubi, and Gerald Quirchmayr. Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology. In *ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, pages 179–186, Washington, DC, USA, 2008. IEEE Computer Society.

[15] BSI (UK). Information securrity management systems – requirements. ISBN 0580467813, 11 2005.

[16] BSI (UK). Business continuity management system – part 1: Code of practice. ISBN 0580496015, 11 2006.

[17] BSI (UK). Business continuity management system – part 2: Specification. ISBN 9780580599132, 11 2007.