Business and IT Continuity Benchmarking

Wolfgang Neudorfer, Louis Marinos, Ingrid Schaumüller-Bichl

Business and IT Continuity Benchmarking

Wolfgang Neudorfer[1], Louis Marinos[2], and Ingrid Schaumüller-Bichl[1]

[1] Upper Austria University of Applied Sciences, Campus Hagenberg,
Department Secure Information Systems
{wolfgang.neudorfer, ingrid.schaumueller-bichl}@fh-hagenberg.at
[2] European Network and Information Security Agency
louis.marinos@enisa.europa.eu

Abstract. The paper introduces a benchmarking approach for business and IT continuity. Multiple use cases of the benchmark are presented enabling organizations of varying sizes and sectors to determine their continuity requirements in a comprehensive manner. Furthermore, the benchmark can be used to compare different business continuity methodologies, but also to identify an appropriate methodology that meets an organization's requirements. This will help organizations to establish and sustain an effective and efficient business continuity process without the need of extended know-how in that area.

Keywords: business continuity management (BCM), risk management (RM), benchmarking, continuity profile, continuity requirements.

1 Introduction

Today's organizations are exposed to numerous sources of threats and vulnerabilities which may have critical impact on their business continuity. In addition, the time after which unavailability may cause irrevocable damage or even threaten the survival of the organization gets shorter and shorter. Therefore, the introduction of a business continuity process that improves the organization's resilience may be of vital importance for an organization.

The establishment and ongoing management of such a process can be both time-consuming and expensive. With the presented benchmarking approach we aim at supporting organizations in understanding both what business continuity is about and what their continuity requirements are. The goal of the paper is enabling organizations of varying sizes and sectors to answer the following questions:

1. What are the continuity requirements for organizations of typical size and complexity?
2. How can an organization determine its continuity profile and identify its basic requirements without prior knowledge in business continuity?
3. How can an organization determine its detailed continuity requirements?
4. How can different business continuity methodologies be compared?

5. How can an organization identify a methodology that meets its own requirements?

The paper is structured according to these questions, whereas Sect. 4 responds to every question with a particular use case of the benchmark.

2 Background

The business continuity process [3] from the European Network and Information Security Agency (ENISA) forms the basis for the current paper. The process depicted in Fig. 1 is being developed as a consolidated overview of relevant methodologies, standards and literature [3, p. 14]. Main objective for the development of this continuity process was to serve as an all-encompassing basis of continuity issues covered by existing approaches. The process has been used for the development of an inventory of continuity methods and tools [4]. Given the properties and due to the independency of ENISA, the process is considered as a solid structure for the presented benchmark.

Figure 1 shows the ENISA business continuity process consisting of six stages[3] and 24 sub-processes. The content of the stages is outlined in the following paragraphs, more detailed information can be found in [3, pp 27-64].[4]

In the first stage the peculiarities of the organization and its environment are identified and responsibilities assigned. The determination of business critical processes, their interdependencies and their supporting assets are considered to be of utmost importance. The BCM policy finally sets out the organization's aims, principles and the approach to BCM.

In the second stage the business impact analysis (BIA) is conducted. The main outcomes from this analysis are the identification of recovery time objectives (RTO), the maximum tolerable period of disruption (MTPD), the recovery point objectives (RPO) and the minimum level of resources needed by critical processes. A recovery profile shows over time what assets are being recovered as well as the specific resources (staff, premises, equipment) that are required at any time to support the recovery efforts.

In the third stage the BCM approach is designed. Given the results from the previous stages, feasible recovery options are developed and a cost-benefit analysis is conducted. Top management finally signs off a business continuity strategy. As a result of this the business continuity plan (BCP) is designed.

In the fourth stage the BCP is delivered. Following ENISA, the BCP is not a single document but rather a suite of documents used by different teams and in different points of time. These documents shall be seen as suggestions, not all of them have to be necessarily implemented.

[3] A stage is considered to be a group of sub-processes.

[4] It should be noted that the scope of the process does not address the continuity of critical business processes itself but rather the continuity of ICT that is needed to provide an automated means for the critical processes. Nevertheless a holistic perspective on the organization is given throughout the process.

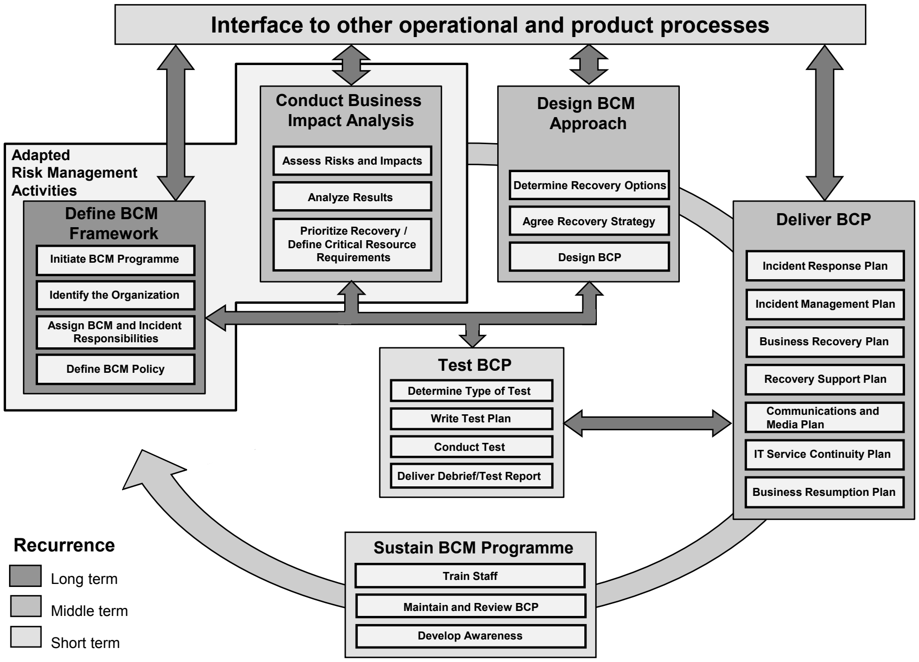

Fig. 1. ENISA business continuity process [3, p.22]

In the fifth stage the BCP is tested. Testing can be achieved through many different test types reaching from simple walkthroughs to complete scenario exercises. Hence, a test plan including scope, timetables and success criteria is worked out.

In the sixth stage the BCM programme is sustained. Modification of the BCP may be necessary due to various reasons reaching from identified shortcomings to changes in the business itself. This stage also ensures that involved personnel are well-trained and capable of handling an incident of unavailability. In addition, it is necessary that all staff is informed about the key principles and that business continuity is embedded in the organizations culture.

3 Benchmarking Approach

In 2007-2008 ENISA has defined a risk assessment and risk management benchmark [5]. The approach followed for risk management has been adopted for the development of the present continuity benchmarking.

The benchmark is built upon the ENISA business continuity process and divides BCM in the same six stages and 24 sub-processes as described in Sect. 2. In addition, the sub-processes are further characterized by information a sub-process needs (i.e. input) and information a sub-process delivers (i.e. output).

While inputs and outputs have been defined for all 24 sub-processes, we do not describe how an input is turned to an output (i.e. processing step). We make the assumption that this can happen in various ways. We have left this information out on purpose in order not to restrict ourselves by means of how a user can best perform a process but what is processed by the process. We believe that this decision is a step towards neutrality of our approach. For the developed benchmark, 87 inputs and 65 outputs have been defined in total.

Due to size limitations we present here for the sake of illustration the inputs and outputs of "P.2 Identify the Organization". The used numbering consists of three parts separated with dots. Starting with an I for input and an O for output, the second part identifies the sub-process the input or output is defined for. The third part is a consecutive number of the inputs or outputs of the particular sub-process.

- Inputs of P.2:
  - **I.2.1** *Business areas of the organization:* A definition of all areas the organization is operating in.
  - **I.2.2** *Strategy of the organization (goals, objectives, strengths, weaknesses, opportunities and threats, culture, structures):* The organizations business strategy is a crucial knowledge for BC planning. Planned mergers or the introduction of new products have a strong influence on BCM.
  - **I.2.3** *Description of internal stakeholders:* An understanding of all internal stakeholders (e.g. employees, business owner, the board) interests and obligations is necessary.
  - **I.2.4** *Description of external stakeholders:* An understanding of all external stakeholders (e.g. shareholder, customer, government, supplier, environment) interests and obligations is necessary.
  - **I.2.5** *Description of assets (inventory list, people, systems, processes, capital, etc.):* The assets of the organization are protected within the BCM against unavailability risks. Their location during normal business operation is an important factor in BCM design.
  - **I.2.6** *Financial and political information:* A definition of the financial and political environment of the organization.
  - **I.2.7** *Relevant legal and regulatory information:* A list of regulations and legislation the organization is faced with.
  - **I.2.8** *Information about geographical, social and cultural conditions:* The geographical position(s) of the organization has/have a big influence on BC planning. Social and cultural conditions can have influences too.
- Outputs of P.2:
  - **O.2.1** *Description of critical business processes and interdependencies between them:* These business processes are critical for the survival of the organization. The identification of critical processes and their interdependencies is of utmost importance. Special attention should be drawn to changes in business (see also I.2.2).
  - **O.2.2** *Assets supporting critical business processes:* Assets that are supporting critical processes are crucial to the organization.

- **O.2.3** *Description of relationships between O.2.1 and O.2.2:* The understanding of the relationships between the assets and the critical business processes is essential to BCM. Attention should be drawn at the interdependencies of the critical processes.
- **O.2.4** *All records of the external environment of the organization:* A summary of the environment of the organization (e.g. external stakeholders, competitors, financial and political information, social and cultural conditions).
- **O.2.5** *List of relevant obligatory laws and regulations (with respect to obligations):* Legal and regulatory information are important as the organization may suffer from liability issues due to an unavailability.
- **O.2.6** *List of key responsibilities and positions inside the organization:* Personnel that will be involved in the handling of unavailability.

A desired side-effect of the defined inputs and outputs of the business continuity process is the development of an integrated approach with a risk management process. As the BC process makes use of risk assessment and risk management techniques, inputs and outputs of the RM process (as defined in [5]) have been re-used to establish an integrated, cost-effective and concise management process for both risk and business continuity. This is considered to be of particular importance because none of either process can be managed in isolation from the other.

For the valuation/rating of inputs and outputs we introduce two concurrently used scales, namely scores and weights. Scores are used to quantify the importance of an input/output, while weights are used to qualify them. The details of scores and weights are as follows:

Scores: Depending on the particular use case, scores indicate the amount of information an input or output should carry. A low score indicates that an input, for example, is only rudimentary described, while a high score indicates that the input is described in great detail. The scoring of the sub-process can be specified by calculating the average of all inputs and outputs of the particular sub-process.

Weighting: Not all inputs and outputs are considered mandatory during implementation of a continuity plan. Some of them are considered to be negligible or not needed yet recommended. As a consequence, a weighting is performed on inputs and outputs.

For better visualization and comparison a radar chart is used for the results of the benchmark. The radar chart can be drawn at the level of sub-processes or at the level of inputs and outputs, depending on the desired detail of visualization. Examples of these charts are shown in Fig. 2 and Fig. 4 respectively later in this paper.[5]

[5] The axes of the chart are scaled to start at -1 to avoid the problem of blank cells should a sub-process have zero score [5, p.6].

4 Use Cases of the Benchmark

In the following section we present five practical use cases of the defined benchmark. These use cases focus on different target groups reaching from managers without deep technical knowledge to experts in business continuity. Use cases 1 and 2 are attractive to non-experts and do not require previous knowledge while use case 3 can be used by a specialist to generate precise results. Use cases 4 and 5 may be used by both, experts and non-experts.

4.1 Use Case 1: Determining Typical BC Organizational Requirements

If an organization decides to establish a BCM process it may wish to understand what typical continuity requirements are. Therefore, this paper defines five characteristic types of organizations [5, p.8]:

1. Small business with limited usage of information and communication technologies (ICT)
2. Small to medium-sized business with more extensive usage of ICT
3. Medium-sized private business with simple governance requirements
4. Medium to large-sized business with more complex governance requirements
5. Large-sized business with rigorous governance requirements

Users of the benchmark can use these characteristic requirements in order to find out how much their continuity profile (see Sect. 4.2) deviates from typical profiles of organizations of the same or similar type.

The benchmark can be used to evaluate the requirements of the types by using the scoring of Sect. 3. The adapted scheme for this use case is shown in Table 1. Figure 2 summarizes the results of the use case and visualizes the performed scoring of all five types in a radar chart.

Table 1. Scoring scheme for use case 1 at sub-process level [6, p.21]

Description	Score
The sub-process is not required for this type.	0
A simple and informal sub-process is required for this type.	1
A formal and documented sub-process is required for this type.	2
A detailed sub-process with full documentation and auditing is required for this type.	3

4.2 Use Case 2: Generation of Continuity Profiles

Obviously, the generic alignment profiles of the first use case cannot exactly describe the requirements of an organization. For a more accurate determination

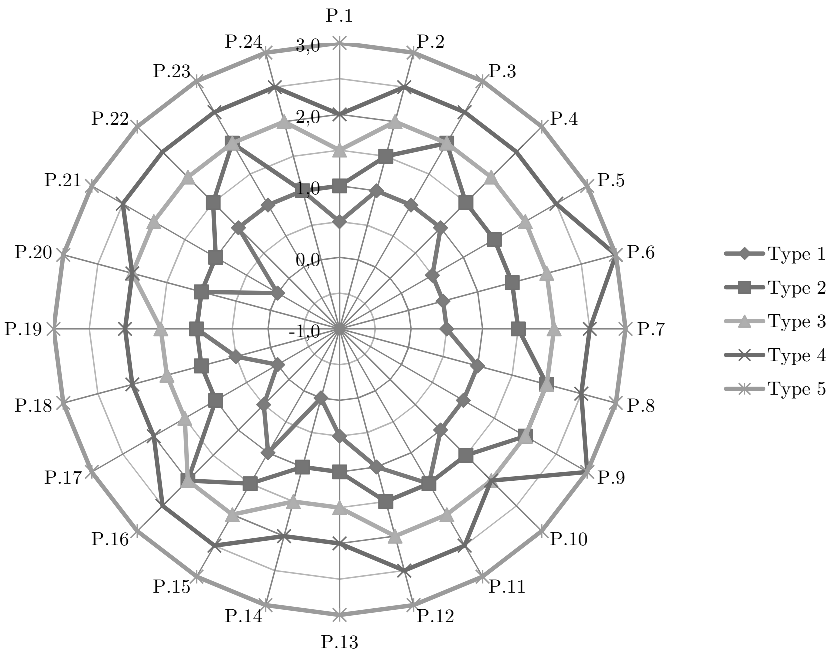

Fig. 2. Typical profiles for organizations of use case 1

the benchmark can be used to identify a more specific continuity profile. Based on the risk profile in [6], the continuity profile is generated through answering a questionnaire focusing on

- the exposure to threats and vulnerabilities (that can lead to an unavailability) and
- the impact of unavailabilities

of the organization. By analyzing the results from the questionnaire each continuity profile provides information about an organization's BCM requirements and gives recommendations as well as additional information for the establishment of a BCM process.[6]

Questionnaire In order to qualify an organization's requirements for BCM the presented approach delivers 14 questions about the exposure to threats and potential sources of vulnerabilities (referred to as "exposure") and the potential impact of these (referred to as "impact"). The questions can be classified in the following sections:

[6] Nevertheless, it should be noted that the identification of a continuity profile shall not be confused with a business impact analysis including detailed risk assessment and risk management methodologies.

- Qualification of exposure:
  - As a result of the organization's nature and its business model
  - As a result of threats
  - As a result of vulnerabilities
- Qualification of impact:
  - As a result of its business strategy and its environment
  - As a result of the organization's legal and regulatory requirements
  - As a result of the organization's dependency on ICT systems

All questions offer the responding organization the option of choosing one of four possible answers. Each question is scored depending on the answer given. The scoring of regular questions is 1-2-3-4 points, while for questions which are of high importance for the continuity profile the scoring is raised to 1-2-4-8 points. To illustrate the approach, one question regarding the exposure (Table 2) and one question regarding the impact (Table 3) are shown as an example.

Table 2. Example question regarding the exposure

(3) - To what extent do you feel that your organization is exposed to natural disasters (e.g. storms, floods, bush fire, earthquakes, hurricanes, pandemic diseases) due to its geographic location(s)?	**Score**
Very little	1
Some	2
Potentially significant	4
Potentially critical	8

Table 3. Example question regarding the impact

(9) - What is the overall tolerable period of disruption for your organization (rough estimate)?	**Score**
1 week or more	1
2 to 4 days	2
less than 1 day	4
less than 4 hours	8

Analysis of the Answers By summing up all scores regarding the exposure and all scores regarding the impact, an *exposure and impact vector* can be created. Through plotting the vector on a xy-chart preliminary indication of the exposure and impact can be given. Figure 3 illustrates the results of an example organization with a scoring of 20 points for exposure and 17 points for impact.

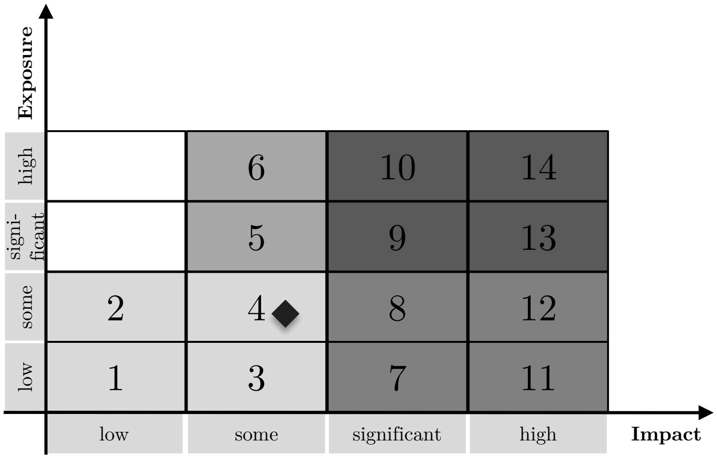

Fig. 3. Exposure and impact vector for example organization: the x-axis represents the impact; the y-axis represents the exposure

Figure 3 also reveals that each axis is divided into four parts, resulting in 14 sectors.[7] For each sector all 87 inputs and 65 outputs are separately evaluated using a similar scoring scheme as in Table 1, but at the level of inputs and outputs. As a result of the scoring and weighting a specific alignment profile for each of the 14 sectors can be drawn by calculating the averages at sub-process level. Table 4 shows the scoring of sector 4 which corresponds to the profile of the example organization.

Table 4. Weighted scoring for sector 4

P.1	**P.2**	**P.3**	**P.4**	**P.5**	**P.6**	**P.7**	**P.8**	**P.9**	**P.10**	**P.11**	**P.12**	**P.13**	**P.14**	**P.15**	**P.16**	**P.17**	**P.18**	**P.19**	**P.20**	**P.21**	**P.22**	**P.23**	**P.24**
1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	0	1	1	1

Determination of Requirements On basis of the previously presented alignment profile general information, levels of concern, requirements, and recommendations of the 14 segments can be expressed. The following listing shows an excerpt of the description of sector 4.

- General information:
  - Organizations of this type may encounter some problems, but these are not likely to be critical to their business.

[7] The approach is adapted from [6, p.10]. Further, [6] concludes that organizations expecting a low impact are unlikely to have significant or high exposure. Therefore, these two sectors have been ignored and are not considered in the plot.

    - If your organization is of this type, you should understand the continuity risk to your business and have regular means of reviewing.
  - Level of concern:
    - The business areas that are critical to the organization shall be identified and responsibilities have to be assigned.
    - Recovery options of critical business areas have to be determined.
  - Requirements: (excerpt)
    - Identify critical business areas and understand their dependencies to ICT.
    - Define RTO and RPO for critical business areas.
    - Develop checklists for the recovery of ICT services.
  - Recommendations: (excerpt)
    - Develop preventative controls for the resilience of critical business areas.
    - All (internal or external) changes that impact the organization are reviewed in relation to business continuity.

4.3 Use Case 3: Detailed Determination of Requirements

The second use case achieves the identification of a convincing continuity profile in very little time and without deep knowledge of the subject matter. However, experts in business continuity may wish to comprehend the characteristics of an organization in greater detail than a questionnaire is able to deliver. For this purpose the benchmark offers the opportunity to self-evaluate all 87 inputs and 65 outputs with the proposed scoring from 0 to 3 points (including intermediate values) in respect to the organization's needs. Also the suggested weighting of the inputs and outputs may be adjusted to the own requirements. Following this approach a very accurate alignment profile can be created.

4.4 Use Case 4: Benchmarking of BC Methodologies

A number of BC methodologies is currently available. Even for experts it is a difficult task to compare the different items and identify their strengths and weaknesses. Applying the scoring scheme shown in Table 5 the benchmark can be used to characterise the methodologies according to the degree of convergence they have to their equivalents in the benchmark.

Table 5. Scoring scheme for use case 4 [5, p.5]

Description	Score
Input/output is not mentioned at all.	0
Input/output described with only reference to an external process.	1
Input/output described in some detail with simple instructions.	2
Input/output described in great detail with exhaustive instructions.	3

For this paper the benchmark has been applied by three different experts to four common methodologies. These are:

- British Standard 25999-1 [2],
- BCI Good Practice Guidelines 2008 [8],
- BSI Standard 100-4 [1] and
- ENISA IT Business Continuity Management: An Approach for SMEs [7].

Furthermore, this paper consolidates the different ratings conducted by the experts and tries to eliminate subjectivity. Using the objective ratings it is again possible to visualize the results of the evaluation in a radar chart and directly compare the strengths and weaknesses of two or more items in a single chart. It should be noted that the comparison can be conducted at the level of sub-processes, or more detailed, at the level of inputs and outputs.

4.5 Use Case 5: Combination of Use Cases

By combining alignment profiles of a particular organization (as in use cases 1-3) and of those of business continuity methodologies (as in use case 4), it is possible to determine an appropriate methodology for the organization. In addition to that, the organization may also wish to select particular sub-processes from different methodologies to achieve best results. For example, although an organization may use the SME approach from ENISA it may decide that its circumstances require more detailed testing of the continuity plans as described in BSI Standard 100-4 [1]. For the sake of illustration, Fig. 4 shows the profile of the example organization and the methodology from ENISA for SMEs [7].

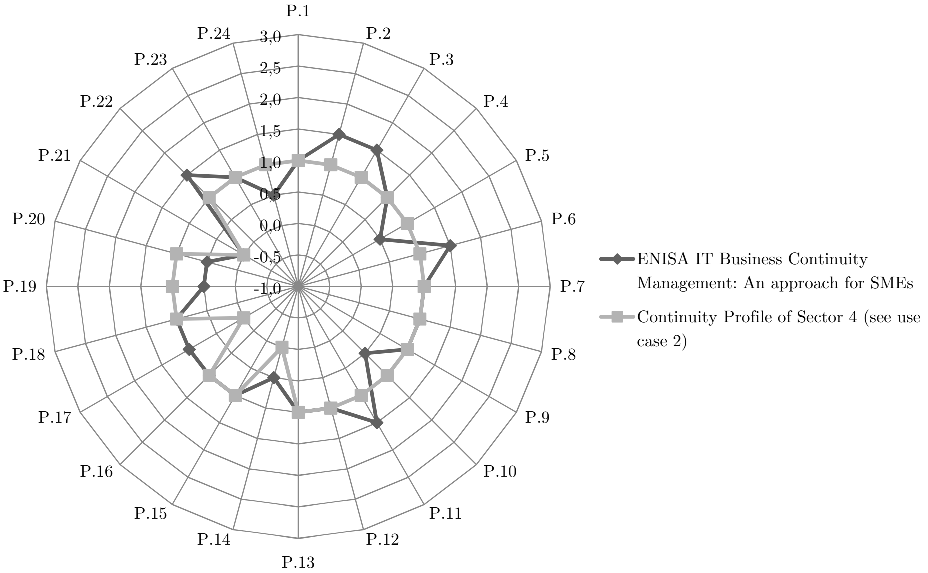

Fig. 4. Continuity profile of the example organization (see use case 2) and a BC methodology (ENISA IT Business Continuity Management: An Approach for SMEs)

5 Conclusion

Availability is a basic principle of communication and multimedia security. A way to proactively improve an organization's resilience against the disruption of its ability to achieve its key objectives is the introduction of a business continuity process [2].

This paper presented a business continuity benchmarking approach. Further, practical use cases showed how the benchmark can be used to determine the continuity requirements of organizations of various sizes and sectors. The use cases also showed how an appropriate methodology for the establishment and ongoing management of a business continuity process can be found.

Future work in this field may include the consolidation of the presented results and the assessment tool *Self Assessed Risk Profiler (SARP)* as introduced in [9]. SARP is able to generate the risk profile for an organization and automatically deliver the appropriate description of its risk assessment and management objectives [6]. The combination of the risk and the continuity profile as well as the comprehensive integration of the risk and business continuity management process (as discussed in Sect. 3) promises to deliver an effective and efficient approach to integrate these related disciplines and make them usable for non-experts and in particular for small and medium enterprises.

References

1. Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Standard 100-4: Notfallmanagement - Version 1.0 (2008)
2. British Standards Institution: British Standard 25999-1:2006 Business Continuity Management - Part 1: Code of practice. (2006)
3. European Network and Information Security Agency (ENISA): Business and IT Continuity: Overview and Implementation Principles. (2008)
4. European Network and Information Security Agency (ENISA): Inventory of Business and IT Continuity Tools. http://www.enisa.europa.eu/act/rm/cr/bcm-resilience/bc-tools
5. European Network and Information Security Agency (ENISA): Methodology for evaluating usage and comparison of risk assessment and risk management items (2007)
6. European Network and Information Security Agency (ENISA): Determining Your Organization's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies. (2008)
7. European Network and Information Security Agency (ENISA): IT Business Continuity Management: An Approach for SMEs (2010)
8. The Business Continuity Institute: Business Continuity Management Good Practice Guidelines 2008 (2007)
9. Pöttinger, J.: Selbsthilfe für IT-Risikomanagement - Ein Benchmarking-Ansatz, 11. Deutscher IT-Sicherheitskongress (2009)