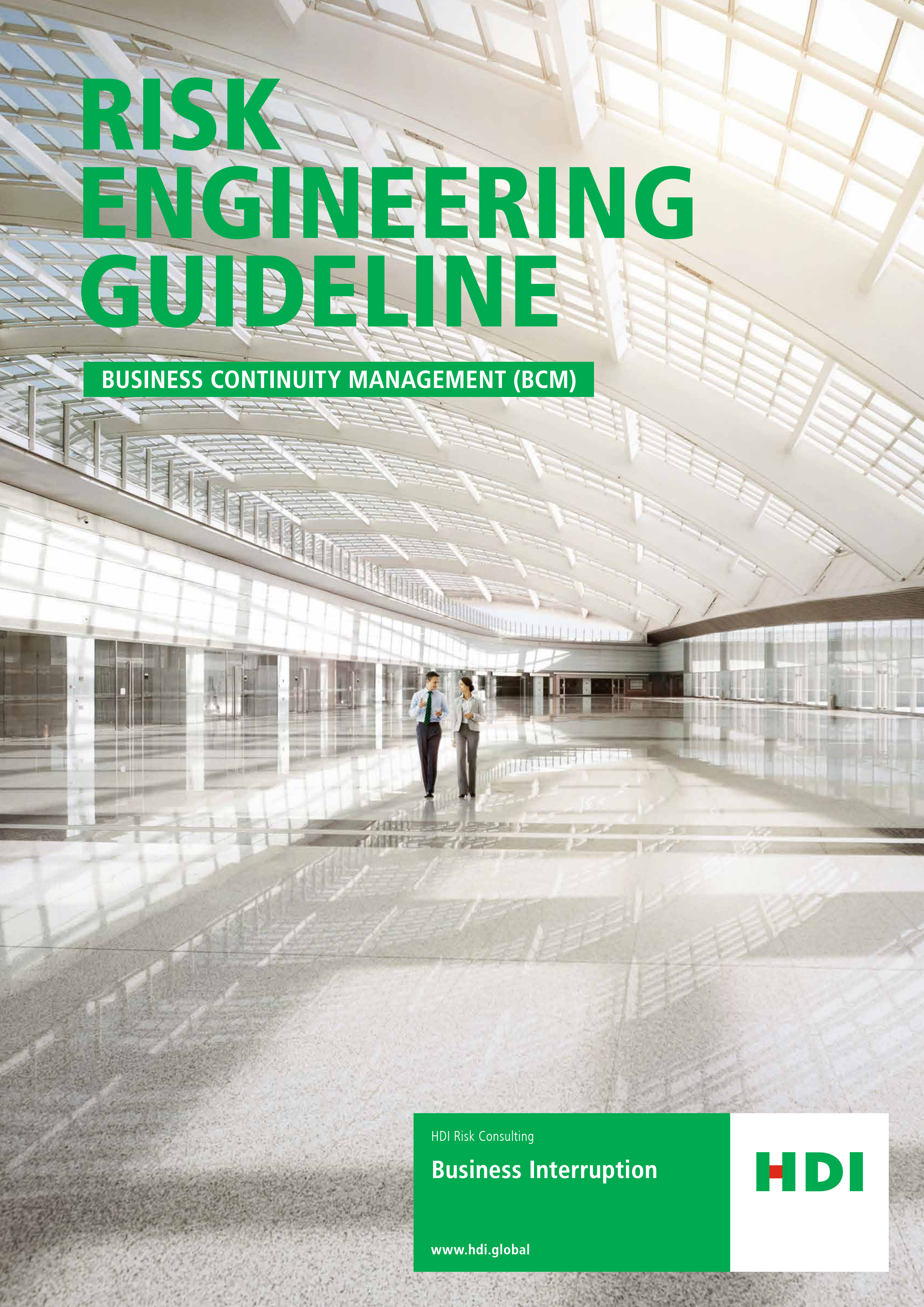

RISK ENGINEERING GUIDELINE

BUSINESS CONTINUITY MANAGEMENT (BCM)

HDI Risk Consulting

Business Interruption

www.hdi.global

Development and Implementation of a Business Continuity Management System (BCMS)

Mitigation of negative impacts and better recovery after a loss event

General.

Existence-threatening Business Interruptions are becoming increasingly important in efficiency-driven and inter-connected value chains. Natural catastrophes, human failure, or large-scale industrial fires may affect value chains around the globe, resulting in substantial production disruptions and financial losses.

As a consequence, companies become more aware of the vulnerability of their supply chains and request their suppliers to improve their risk management. At the same time, regulatory requirements regarding the identification and mitigation of existence-threatening risks are continuously increasing.

However, not all risks can be eliminated proactively and may result in substantial financial losses, if the situation is not adequately managed. Hence, there is a need for companies to prepare for such incidents in order to mitigate negative impacts on their business.

Business Continuity Management (BCM) is a management system, which if implemented correctly, will allow a company to recover better from major losses of infrastructure and resources in a systematic and structured way. Therefore, the impact of an incident shall be reduced to an "acceptable" level, to ensure a defined service level is maintained and recovery is accelerated.

The client base will therefore be better protected, regulatory requirements met and financial losses reduced.

Example

At the production location of a midsized company a fire started in the air preheating unit of the main oven. Firefighting activities were cautious to avoid additional water or powder extinguishing agent damage. Due to a lack of further combustible materials, the fire did not spread.

The outcome was a total loss of the whole unit consisting of the main oven and several auxiliary units including the central process control. Replacing the lost equipment was not straight forward as the installation had been built and adjusted through several decades by several engineers with no historical data retained detailing the design of the alterations. A further complication was the fact that this was not a commodity business, so there was no possibility of an "off the shelf" solution. Hence, the whole installation would have to be redesigned and engineered. It took weeks to arrive at this conclusion and the customers had to be informed that there would be no supply of goods within a time period of at least 12 months.

The design process took several months and it was 9 months post loss before the manufacturing of the new unit commenced. Production restarted almost two years after the loss. The insurance policy had an indemnity period of 24 months and although the company managed to retain a few loyal clients, the majority were lost to competitors.

In technical terms, the indemnity period was sufficient to meet the recovery time of the business. However, the major market losses continued, ultimately threatening the survival of the whole business.

Had the gap in knowledge and design data been identified and recovery strategies developed pre-incident i.e. as part of the BCMS planning process, the timescale for recovery could have been reduced to a level that would have prevented the excessive loss of market share and ultimate failure of the business.

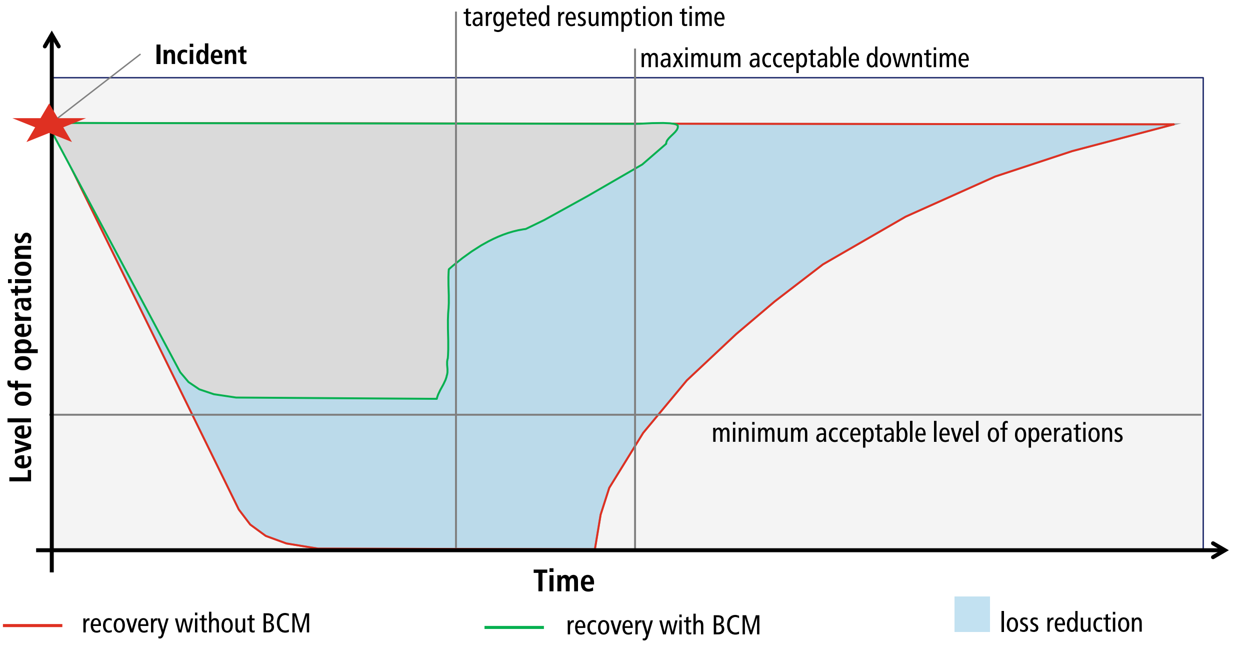

Fig. 1: In the loss example above, the incident happened and followed the red line in the table above. The business recovered from the incident but recovery was outside the targeted resumption time and below the minimum acceptable level of operations by the time they reached the maximum acceptable downtime. Undertaking a BCM process would have established all these parameters and highlighted any necessary actions required e.g. reverse engineering to produce drawings and specifications for the critical production equipment to ensure recover of these critical elements could be established within the identified timescales.

1 Process.

The establishment of a BCMS can be best explained by following the BCM lifecycle. The lifecycle means that once the different elements of the cycle are defined and implemented, BCM is an ongoing process and should be reviewed annually.

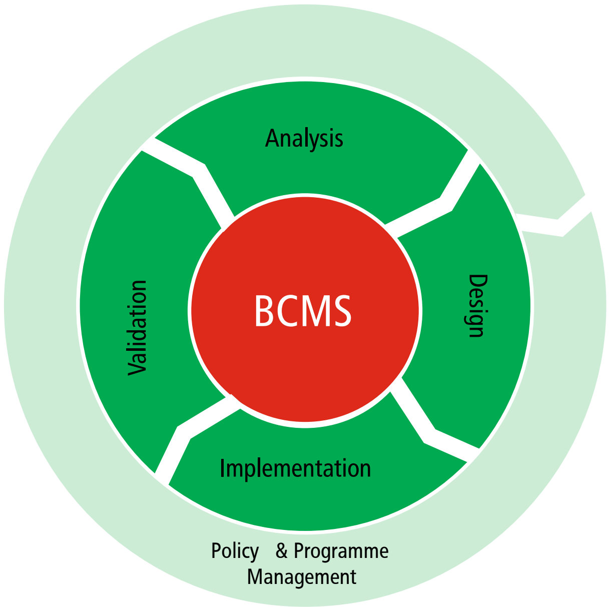

Fig. 2: BCM Lifecycle.

1.1 Policy & Programme Management (BCM Policy)

Establishing the policy provides the organizational structure for all further BCM activities and requires the involvement of senior management. The first step is to define the scope of the BCMS. What is the protection target, which areas of the company – depending on your business objectives – shall be included? Senior management input will be required for these strategic, operational and tactical responses which should all be fully documented.

The next step will be to build the organizational structure and process of the BCMS, i.e. identifying roles and responsibilities; deciding methodologies for Business Impact Analysis (software tool/inhouse/consultancy), prioritizing the implementation; establishing any possible interfaces with existing management systems; setting budget, governance and timelines.

Therewith, the policy is the guideline for all further BCM activities and requires the approval of the top management.

Recommendations

- Start with a small scope and expand it later.
- Don’t forget to get the explicit support by senior management.
- Answer the question: what are the crucial processes for the survival of the company?

The programme management needs also to be specified in the policy and assures the functionality of the BCMS: as companies develop and the environment changes, the BCMS has to be adapted continuously to new situations and requirements.

Therefore, a yearly control of the policy, critical processes, Business Continuity Plans (BCPs) and strategy options is essential. If major changes occur in the meantime, the cycle might also be adapted.

However normally, there should be yearly test intervals for the BCPs. Not all BCPs have to be tested every year, but a certain percentage should be tested to assure continuous improvement.

Over the years, the assumptions, content and testing should be reviewed, and the scope of the BCMS can be extended where required.

Note: each BCMS is different, as it has to be designed specifically to meet the requirements and characteristics of the organization in question. Therefore, copying a BCMS from another organization is in general not useful.

1.2 Analysis

The analysis stage provides the focus and direction for the remainder of the process. It divides into two separate but interrelated streams – BIA (Business Impact Analysis) and TE (Threat Evaluation).

The BIA requires the specific knowledge of all relevant departments, their involvement in the analysis is of paramount importance. Within the agreed scope, the (time-) critical processes have to be identified together with the impact their loss would have on the business. Furthermore, the resources, activities and supporting processes required for each critical process have to be determined as well.

Recommendations

- Start with a short explanation, what has to be done and why and issue an identical template to all departments with identical impact measurement categories.
- The critical processes shall be named, their function (briefly) explained and the potential (financial / operational / reputational) impact of their loss assessed.
- Don’t forget to ask for what else is required to keep the process running.

The clarity and accuracy of collated data is essential for an effective continuity programme. Once the data is established, it is necessary to identify what could threaten the continuation of those critical processes – which is done by the TE.

Hence, the risks surrounding the process have to be analysed. This TE should be done for each location separately, as the risk environment changes with each location. Risks to be considered are e.g. natural hazards, fire, single points of failure, etc. by using a matrix of probability (of the threat occurring) and severity (relevant to your operation) a risk factor is produced.

Recommendations

- The threat evaluation should include walk-throughs by qualified personnel regarding fire protection, work safety, security, etc..
- These walk-throughs give also insights on potentially feasible mitigation strategies per location.
- Risk reports and Business Interruption analyses by the property insurer might assist in facilitating the BIA and TE.

1.3 Design

Using the information from the first two stages, it is now possible to develop recovery strategies and threat mitigation measures. The choice of strategy depends on a series of criteria, e.g. feasibility, practicability, budget and potential regulatory constraints.

The strategy can be defined e.g. per location, process or resource. It has to take into consideration the specific influencing factors and may differ e.g. per location.

For instance, at one site there might be the option to move assembly into nearby empty buildings, whereas at other locations, the only feasible option might be to source the service externally. The available budget might also depend on the criticality of the process for the overall business model of the company. Thereby, less probable risks should not be neglected altogether, as those incidents are frequently the most existence-threatening ones.

For the recovery of each critical process, questions have to be answered regarding the maximum acceptable downtime and the minimum acceptable level of operations, regardless of the cause of the incident. Furthermore, the recovery strategies should be as consistent as possible to avoid increased workload and expenses.

Threat mitigation measures should be developed and implemented to reduce the key threats identified at the analysis stage. For example, to mitigate significant flood risk, key machinery could be repositioned onto raised plinths or fitted with hydraulic jacks to raise off the floor when necessary. Thereby, the amount of BCPs to be developed might be reduced.

1.4 Implementation

This stage is about documenting the tasks, responsibilities, decisions and priorities required to execute the plan.

For the implementation of BCPs, roles and responsibilities have to be defined and attributed to the respective person.

During a critical situation, the Business Continuity Plans (BCPs) have to be understood and executed. Hence, they should be written as clearly and concisely as possible. Important supporting information includes accurate and up-to-date contact details of team members, responsible coordinators and other relevant people or authorities. Required resources need to be described and their storage location identified e.g. 'battle box' containing hard hats; hi-vis vests; 2-way radios; stationery etc.; the base location for the recovery response team and so on.

The BCPs shall answer the questions:

- What?
- When?
- Where?
- Who?
- How?

Furthermore, it should be clear when it is appropriate to activate the BCPs and how to escalate as the incident develops.

It is not the intention for the BCPs to cover every eventuality and procedures may need to be adapted to cater for the specific incident. The recovery response team must include personnel with adequate authority to make these decisions, as well as experts of the process to be recovered.

1.5 Validation

Validation of BCPs through testing, maintenance and review is crucial to the success of BCM. This is where the recovery strategies developed in the 'Design' stage are substantiated or refuted and amended. Different levels of test can be practiced depending on the maturity of the BCMS, from desktop exercises to full, live simulations.

It has to be considered that the more sophisticated the plan tests become, the greater the budget and resources required. Live tests are extremely valuable, but require substantial preparation to avoid unforeseen business interruptions due to testing.

Recommendations

- Different levels of tests should be used depending on maturity of BCMS.
- They should not be too complex at beginning to create positive feedback.
- More mature tests might be conducted with external service providers.

Example

During a full simulation exercise a client wanted to include a test of their call-out cascade procedure. The exercise was initiated using their emergency contact number. The response was an answerphone message referring the caller to another number which in turn referred the caller to the original emergency contact number.

The fault could have caused significant delay to proceedings in an emergency situation. The fact that this fault was identified during a plan test meant it was able to be corrected allowing any future invocations to flow smoothly through this element of the plan.

2 Establishment of BCMS.

Embedding the culture of BCMS requires organisational acceptance, a good standard of communication, and support from senior management. Hence, a "BCM culture" has to be established.

Throughout all phases of the lifecycle, information and communication of the contents and goals of BCM are key to achieving "buy-in" from all concerned.

This is not an unfamiliar concept as most businesses have other subjects that require embedding into the organisational culture i.e. Health & Safety; Quality Standards etc.

Regular communication should be established e.g. information campaigns; activity weeks; newsletters; notice board posters; team talks. The topic should be a regular feature for management and board meetings.

As can be seen, the development and implementation of a BCMS requires thorough preparation, foresighted decisions and accurate documentation. However, the result can make the difference between a temporary setback and an insuperable loss of business.

3 References.

1. BSI Standard 100-4: Business Continuity Management
2. ISO 22301: International Standard for Business Continuity Management – Requirements
3. ISO 22318: International Standard for Business Continuity Management – Guidelines

3 BCMS Checklist.

The checklist below provides a brief overview of each of the BCMS phases. This may be used as a maturity check whether an existing BCMS covers all necessary aspects.

Writing the policy:

- Has the top management declared its support and provided the funds necessary to establish and maintain a BCMS? □
- Has the regional/organizational scope been defined? □
- Are the BCM roles named, responsibilities described and attributed to members of the organization? □
- Has the proceeding been described? □

Execution of the Business Impact Analysis:

- Are the time critical processes identified for each regional/organizational unit within the scope of the BCMS? □
- Has the impact of the non-availability of the process been assessed? □
- Have supporting processes, required resources and activities for these critical processes been identified and documented? □
- Have potential interdependencies of critical processes been identified? □

Execution of the Risk Assessment:

- Have Risk Assessments been conducted for each location within the scope of the BCMS? □
- Have risk factors been identified, which could result in disruptions of critical processes? □
- Have strategy options for every location been identified, which could be used to recover critical processes? □

Design and Implementation of BCPs:

- Have mitigation measures been chosen for non-availability of each critical process? □
- Are the incidents response teams defined, members named and contact details provided? □
- Are roles and responsibilities written down, including the clear activation procedure of the decision authorities? □
- Are activities named and prioritized? □
- Are required resources named and is their location clearly described? □
- Is the procedure described for resuming normal operations? □

Validation of BCPs:

- Is there a test program defined for all BCPs? □
- Are exercises conducted regularly? □
- Do exercises vary in kind and complexity? □
- Are the BCPs tested against measurable criteria? □
- Are the results of tests documented? □

Establishment of BCMS:

- Are the goals of BCM clear and according to the vision and mission of the company? □
- Are employees regularly informed about the BCMS and its value-added for the company? □
- Is the management regularly informed about the progress and insights of the BCMS and is its ongoing support assured? □

Program Management:

- Are the components of the BCMS controlled at least once a year and adapted if necessary? □
- Is the suitability of the scope assessed regularly and expanded if necessary? □
- Is there a feedback loop between the test results and the contents of policy and BCPs? □
- Is the BCMS checked and if necessary adapted in case of major changes in the company? □

About HDI Risk Consulting.

HDI Risk Consulting GmbH supports major corporations, industrial and mid-size companies with loss prevention and in establishing risk management systems.

HDI Risk Consulting offers its’ customers access to some 180 engineers and experts from a wide range of technical disciplines. We aim to support companies with the management of risks and the development of individual risk-based concepts for insurance cover.

HDI Risk Consulting operates globally in the Property, Motor, Engineering and Marine markets, with particular focus on the identification and assessment of risks and the development of appropriate, individual protection concepts.

HDI Risk Consulting GmbH is a wholly owned subsidiary of HDI Global SE.

HDI Risk Consulting GmbH
HDI-Platz 1 - D-30659 Hannover
Phone: +49 511 645-3219
Fax: +49 511 645-4542
Internet: www.hdi.global

Imprint
Responsible for the content:
HDI Risk Consulting GmbH

Layout: Insignio Kommunikation GmbH
Fotos: Fotolia, gettyimages, istock

Although we made every effort possible to ensure the accuracy of the information provided, no liability can be assumed for the currentness, correctness and completeness of the information. We neither intend, nor assume any obligation, to update or revise these statements in light of developments which differ from those anticipated.