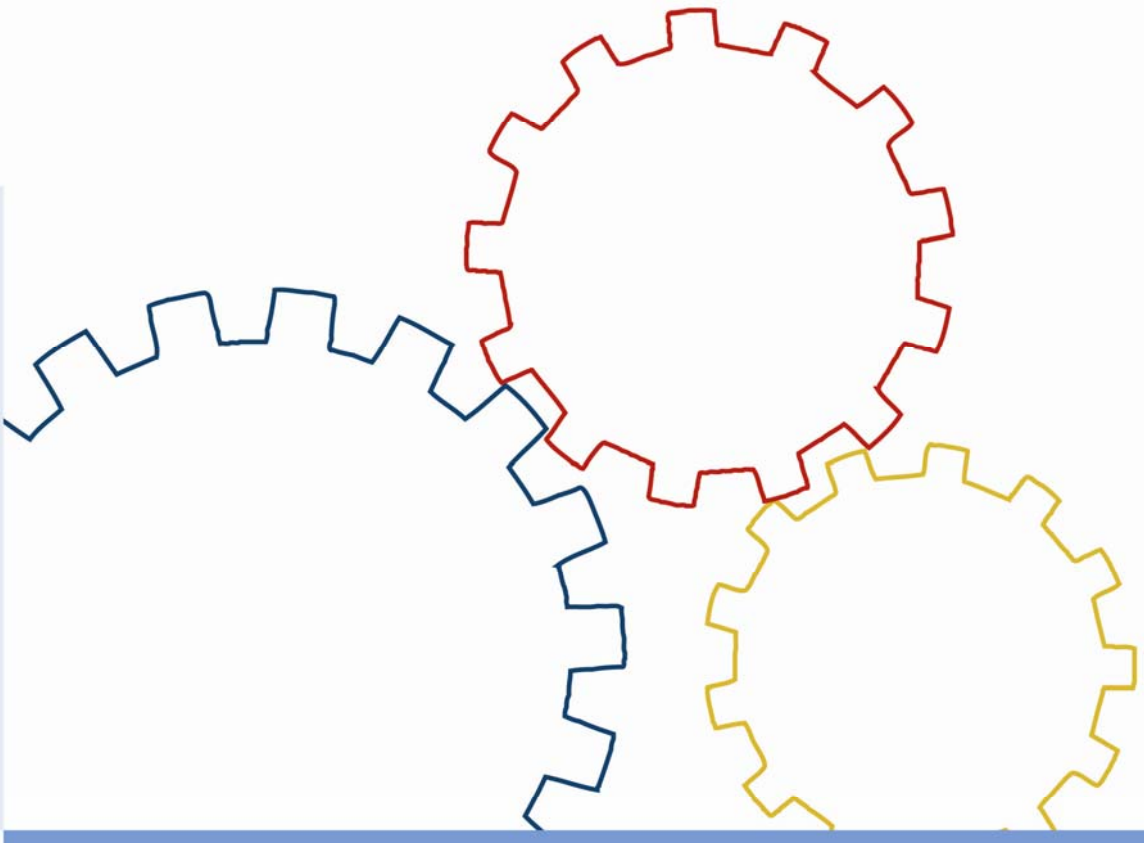
Federal Office
for Information
Security

BSI-Standard 100-4

Business Continuity Management



www.bsi.bund.de/grundschutz

Version 1.0

Federal Office for Information Security (BSI)

Godesberger Allee 185-189, 53175 Bonn, Germany

Table of Contents

1 Introduction

1.1 Version history

As per	Version	Author
November 2008	1.0	BSI

1.2 Aims

Government agencies and companies are exposed more and more to risks that endanger productivity or the ability to provide their services to their customers promptly and continuously. Various developments and trends in society and the economy contribute to these risks, for example increasing globalisation, networking, centralisation, automation, outsourcing, or offshoring. Due to the increasing complexity of business processes and their rising dependency on information technology and external service providers, events such as fires, floods, or the loss of information technology, service providers, suppliers, or personnel can have a significant impact. Furthermore, the risk of pandemics, extreme weather conditions, and terrorism is also increasing.

Business Continuity Management (BCM) is a management process with the goal of detecting serious risks that endanger the survival of an organisation early and to implement safeguards against these risks. To ensure the operability, and therefore the survival, of a company or government agency, suitable preventive measures must be taken to increase the robustness and reliability of the business processes as well as to enable a quick and targeted reaction in case of an emergency or a crisis. Business continuity management consists of a planned and organised procedure for sustainably increasing the resilience of (time-)critical business processes of an organisation, reacting appropriately to events resulting in damages, and enabling the resumption of business activities as quickly as possible.

The goal of business continuity management is to ensure that important business processes are only interrupted temporarily or not interrupted at all, even in critical situations, and to ensure the economic existence of the organisation even after incurring serious damage. A holistic approach is therefore critical in this regard. All aspects necessary for maintaining the continuity of the critical business processes when damage is incurred should be examined, not only the aspect of information technology resources. IT-service continuity managementis a part of business continuity management.

In this standard, BSI Standard 100-4, a methodology for establishing and maintaining an agency-wide or company-wide internal business continuity management system is presented. The methodology described here builds on the IT-Grundschutz methodology described in BSI Standard 100-2 [BSI2]. By fully implementing this standard and the corresponding modules in the IT-Grundschutz catalogues, as a business continuity management system that also completely fulfils the less technically-oriented standards like the British standard BS 25999 Parts 1 and 2 can be established.

The “Critical Infrastructure Protection in Germany” project [KRI] was initiated to meet the challenges posed to agency-wide or company-wide emergency or crisis management. The project was implemented in the form of the “CIP Implementation Plan” and “Implementation Plan for the Federal Administration”, among other plans. External emergency and crisis management in the sense of disaster recovery is the task of the “Federal Office of Civil Protection and Disaster Assistance” (BBK) and has the goal of guaranteeing public and civil protection. Neither of these two subjects are handled in this BSI standard and are considered supplemental subjects.

1.3 Target group

This document is aimed at emergency or business continuity managers, crisis team members, the people responsible for security, security officers, security experts, and security consultants who are familiar with managing emergencies and crises of technical and non-technical origin. Users of the methodology described in this document should be familiar with the IT-Grundschutz methodology

described in BSI Standard 100-2.

Appropriate business continuity management is necessary in small organisations as well as large organisations. Effective and suitable business continuity management does not need to be expensive. Since small and medium-sized organisations are generally less complex, are distributed among fewer locations, have fewer business processes, and are subject to fewer dependencies, the costs for business continuity management are correspondingly lower. However, the existence of precisely these kinds of organisations is endangered when their business processes malfunction, even if the malfunction is minor.

BSI Standard 100-4 is written so that the methodology can be used by organisations of any type or size and from any industry. It completely describes the optimal method of implementation and is directed towards large organisations. Note, though, that all recommendations should be examined and appropriately implemented in the context of the particular organisation. Small and medium-sized organisations should follow the essential substeps and subtasks after modifying them accordingly.

1.4 Application

This document describes a methodology for establishing a business continuity management system based on and extending upon the procedure for implementing a management system for information security described in BSI Standard 100-2 [BSI2]. By using the data acquired when implementing IT-Grundschutz, it is possible to utilise synergy effects and save costs.

It is recommended to apply the methodology described in Chapters 4 through 9 of this standard step-by-step. In particular, it must be pointed out that business continuity management should not be viewed as a project and can only be considered to be effectively implemented when the steps in the process are performed repeatedly.

The term "organisation" is used in this document as a general term for companies, government agencies, and other public and private organisations.

All personal pronouns used in this document refer equally to men and women. The male form of a term is only used in the text when this makes the document easier to read.

1.5 References

[BMIKI] Federal Ministry of the Interior (BMI), Protecting Critical Infrastructures – Risk and Crisis Management, a guide for companies and government authorities, www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfade n Schutz kritischer Infrastrukturen,templateId=raw,property=publicationFile.pdf/Leitfaden Schutz kritischer _Infrastrukturen.pdf, Dec. 2007

[BMIKK] BMI, Federal Ministry of the Interior: Crisis Communication – A guide for government authorities and companies, www.bmi.bund.de, 2008

[BSI1] Federal Office for Information Security (BSI), Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, June 2008, www.bsi.bund.de/

[BSI2] BSI, IT-Grundschutz Methodology, BSI Standard 100-2, Version 2.0, June 2008, www.bsi.bund.de/

[BSI3] BSI, Risk analysis based on IT-Grundschutz, BSI Standard 100-3, Version 2.5, June 2008, www.bsi.bund.de

[BSIHVK] BSI: High Availability Compendium, Version 1.0, published in the first quarter of 2009

[BSIKRI] BSI: Critical Infrastructure Protection in Germany. www.bsi.de/fachthem/kritis/index.htm

[BS259991] British Standards Institute, BS 25999-1:2006 Business Continuity Management, Part 1: Code of practice, www.thebci .org/standards.htm

[BS259992] British Standards Institute, BS 25999-2:2007, Business Continuity Management, Part 2: Specification, www.thebci .org/standards .htm

[GPG08] Business Continuity Institute, Good Practice Guidelines 2008, www.thebci. org/gpgmoreinfo.htm

[GSK] BSI, IT-Grundschutz Catalogues – Standard Security Safeguards, published annually, www.bsi.bund.de/gshb

[HB221] Standards Australia, Business Continuity Management, ISBN 0-7337-6250-6, 2004

[INS24001] Standards Institution of Israel, INS 24001:2007, Security and continuity management systems - Requirements and guidance for use, 2007

[ITIL] Office of Government Commerce, IT Infrastructure Library, Service Management - ITIL (IT Infrastructure Library) www.ogc.gov.uk/guidance_itil.asp, Jan. 2008

[ISO20000] International Organisation of Standardization (ISO), ISO/IEC 20000, IT Service Management; consisting of ISO/IEC 20000-1:2005, IT Service Management - Part 1: Specification for Service Management ISO/IEC 20000-2:2005, IT Service Management - Part 2: Code of Practice for Service Management

[ISO22399] ISO, ISO/PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management

[ISO27001] ISO, ISO/IEC 27001:2005 information technology - Security techniques - Information security management systems requirements specification, ISO/IEC JTC1/SC27

[ISO27002] ISO, ISO/IEC 27002:2005 Information technology – Code of practice for information security management, ISO/IEC JTC1/SC27

[NIST34] National Institute of Standards and Technology (NIST), NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002, csrc.nist.gov/publications/nistpubs/

[NFPA1600] National Fire Protection Association, Standard on Disaster/Emergency Management and Business Continuity Programs, 2007, www.nfpa.org

[PAS77] British Standards Institute, PAS 77:2006, IT Service Continuity Management - Code of Practice, www.standardsdirect.org/pas77.htm

[SS540] Singapore Standard, SS 540:2008, Business Continuity Management (BCM), SPRING Singapore, www.spring.gov.sg

2 Business Continuity Management and IT-Grundschutz

2.1 Classification within the BSI standards

BSI Standard 100-1 [BSI1] specifies general requirements for a management system for information security (ISMS), which also includes generic requirements for business continuity management. BSI Standard 100-2 [BSI2] presents the IT-Grundschutz methodology, a method for establishing and operating an ISMS in practice. The structure of a security organisation and how it is embedded in the organisation are important subjects of these standards. This also includes its interaction with the business continuity management organisational structure. BSI Standard 100-3 [BSI3] presents a method for performing a risk analysis that is optimised for use with the IT-Grundschutz methodology.

This standard, BSI Standard 100-4, builds on the previous standards but describes a stand-alone management system for business continuity and business continuity response. The goal of this standard is to point out a systematic method for enabling fast reactions to emergencies and crises of all types and origins that could lead to a disruption of business operations. It describes more than just IT service continuity management and therefore should not be viewed as a subset of ISMS. BSI Standard 100-4 describes how the results of the classic IT-Grundschutz methodology performed according to BSI Standard 100-2 and the risk analysis according to BSI Standard 100-3 can be used as a basis for appropriately preventing and avoiding emergencies as well as a basis for minimising the damages resulting from an emergency. It points out the need to co-operate closely with security management to establish efficient business continuity management in an organisation. The more intensely the business processes utilise information technology, the more synergy effects can be gained through co-operation with the ISMS. Close co-operation between these two disciplines is recommended due to the large number of overlapping areas of responsibility.

The business impact analysis (BIA) described in this standard is introduced as an additional tool for performing the protection requirements determination according to the IT-Grundschutz methodology. With the help of the BIA, the critical business processes are identified and the availability requirements for the processes and their resources are determined.

Information security management focuses on protecting the information in an organisation while business continuity management focuses on the critical business processes. The information in an organisation is considered to be a valuable resource requiring protection (also referred to as assets), and the critical business processes form the backbone of an organisation. Both management systems apply a holistic approach. The business areas are the drivers behind business continuity management as well as information security management.

2.2 Terms

Disruptions of business processes can have different causes and different effects. To illustrate which events are to be considered in the framework of business continuity management, we provide short explanations of the terms “malfunction”, “emergency”, “crisis”, and “disaster” as they are understood and used in the framework of this standard.

Malfunction

A malfunction is a situation in which the processes or resources of an organisation do not operate as intended. The damages resulting from a malfunction are to be considered “low”. “Low” damage in this sense is damage that is negligible in comparison to the annual results of a company or the total budget of a government agency, or that only has a minor effect on the ability of the company or government agency to perform its tasks. Malfunctions are generally eliminated while performing the daily troubleshooting procedures integrated into routine business operations. However, malfunctions can escalate to an emergency and must be observed critically, documented carefully, and eliminated promptly.

These tasks are not the responsibility of business continuity management, though, and are instead the responsibility of fault management.

Emergency

An emergency is a event in which the processes or resources of an organisation do not function as intended. The availability of the corresponding processes or resources cannot be restored in the required time frame. Business operations are seriously affected. It may be impossible to uphold any existing SLAs (Service Level Agreements). The resulting damages are high to very high and affect the annual results of a company or the ability of a government agency to fulfil its tasks so significantly that such damage is unacceptable. Emergencies cannot be handled during general daily business operations and require a special business continuity response organisation instead.

Crisis

A crisis is understood to be a situation deviating from the normal state which can occur at any time in spite of the preventive safeguards implemented in the company or government agency and which cannot be handled by the normal organisational and operational structures. Crisis management is activated in this case. There are no procedural plans for responding to crises, only general instructions and conditions. A typical feature of a crisis is the uniqueness of the event.

Emergencies that can adversely affect the continuity of business processes can escalate and become crises. A crisis in this case is understood to be a serious emergency in which the existence of the organisation or the health and lives of people are at risk. The crisis is concentrated on the company or government agency and does not have a widespread affect on the environment or public life. A crisis can be managed, at least for the most part, by the organisation itself.

However, there are a number of crises that do not affect the business processes directly. Examples of such crises are economic crises, management crises, liquidity crises, fraud, product extortion or abuse, kidnapping, and bomb threats. The crises examined in the framework of this standard represent a subset of these crises.

Disaster

A disaster is a large-scale damaging event that is difficult to restrict locally and chronologically and that has or can have wide-ranging effects on people, assets, and property. The existence of the organisation or lives and health of people are at risk. Public life is also seriously affected. A disaster cannot be handled by the organisation alone. In particular, disaster recovery teams are needed due to the geographic spread of a disaster and its effects on the population. This is the responsibility of the states in Germany, with support provided by and expanded upon by the federal government. From the organisation's point of view, a disaster is considered to be a crisis and is handled internally by the business continuity response team of the organisation in co-operation with the external aid organisations.

2.3 Other standards for business continuity management

The subject of business continuity management is handled in various standards as well as in national and de-facto standards. Some standards are presented briefly in the following. The list is by no means complete.

BS 25999-1 / BS 25999-2

BS 25999-1 "Business Continuity Management - Part 1: Code of Practice", published in November of 2006 by the British Standards Institute, describes the structure of management system for business continuity management [BS259991]. This includes, among other items, the organisational structure, implementation of a business continuity management process based on codes of good practice, and the organisational safeguards concept. The detailed steps to take or specific safeguards to be implemented for business continuity management are not described. The reader is referred to other standards such as ISO 27001, ISO 20000, or PAS77 for this purpose.

The British standard BS 25999-2 "Business Continuity Management - Part 2: Specification" specifies the requirements that must be fulfilled for certification of a business continuity management system [BS259992].

The core of a business continuity management system according to BS 25999 is program management, which is the control element assigning the areas of responsibility and ensuring permanent operability of the business processes. The life cycle of the BS 25999 consists of four phases:

- Obtain comprehensive knowledge (transparency) of your own organisation (e.g. by performing a BIA and a risk analysis)
- Development of BCM strategy options
- Development and implementation of reaction measures and BCM plans
- Performing BCM exercises and examining and refining the BCM plans and BCM safeguards.

Support is to be provided to these four phases by establishing a BCM culture in the organisation.

Good Practice Guidelines (GPG)

Another BCM guideline is the "Good Practice Guidelines" (GPG) from the Business Continuity Institute (BCI) [GPG08]. The BCI was founded in 1994 and has more than 4000 members in over 85 countries (as of February 2008). Its goal is to set a high standard for business continuity management and become an authority in this area.

The Good Practice Guidelines were published for the first time in 2002. It was developed by the BCI members and has been updated and optimised regularly since then. The GPG has been translated into several languages. The German translation is from 2005.

The BCI GPG 2008 is divided into six sections:

Section 1: BCM Policy & Program Management (development of the BCM policies and process management)

Section 2: Understanding the Organisation

Section 3: Determining the BCM Strategy

Section 4: Developing and Implementing BCM Responses

Section 5: Exercising, Maintaining, & Reviewing BCM Arrangements

Section 6: Embedding BCM in the Organisation's Culture

With more than 120 pages, the GPG from the BCI, as one of the few quasi-standards, offers a real implementation aid for implementing business continuity management in an organisation.

ISO / PAS 22399

The preliminary norm ISO/PAS 22399 "Societal security - Guideline for incident preparedness and operational continuity management" was published in 2007 [ISO22399]. This preliminary norm describes in 31 pages the process and the principles of "Incident Preparedness and Operational Continuity Management" (IPOCM) in a generic way common to ISO standards.

The IPOCM life cycle is divided into the following phases:

- Policy
- Planning
- Implementation and operation
- Performance assessment
- Management review

The IPOCM life cycle contains all the steps in the BCM life cycle. The term "IPOCM" is therefore understood to be an extension of the term "BCM".

The preliminary norm is based on the NFPA 1600 [NFPA1600], HB 221:2004 [HB221], BS 25999-1:2006 [BS259991], INS 24001:2007 [INS24001] standards and on Japanese regulations. The special feature of this norm is the target group. Companies are addressed, of course, but it focuses especially

on private and public organisations as well as administrations.

ISO 27001 / ISO 27002

Due to the complexity of information technology and the demand for certification, numerous manuals, standards, and norms for IT security have emerged over the past several years. ISO/IEC 27001 “Information technology - Security techniques - Information security management systems requirements specification” [ISO27001] is the first international standard for information security management that also permits certification. ISO/IEC 27001 provides general recommendations on about 10 pages. The security recommendations (controls) from ISO/IEC 27002 are referred to in a normative annex. However, the reader is not provided with any assistance for the practical implementation.

The ISO/IEC 27002 (previously ISO/IEC 17799) standard “Information technology - Code of practice for information security management” [ISO27002] is a collection of experience, procedures, and methods gained from practical applications. Its goal is to define a framework for information security management. The standard is therefore primarily concerned with the steps necessary for developing a security management system and for integrating this securely in the organisation. The corresponding security recommendations are sketched briefly on about 100 pages. Chapter 14 of ISO/IEC 27002 is concerned with the subject of business continuity management (BCM). The five pages in this chapter containing recommendations for BCM in the framework of security management are very generic and describe the most important process steps to take at the management level.

NIST SP 800-34

The NIST SP 800-34 standard “Contingency Planning Guide for Information Technology Systems” published in 2002 by the National Institute of Standards and Technology (NIST) is a guide for contingency planning for IT systems [NIST34].

The NIST SP 800-34 standard describes a methodology for structuring an IT contingency planning organisation, the selection and implementation of safeguards for IT contingency planning, and how to handle emergencies on about 60 pages. Specific approaches to a solution are provided in some sections. Templates can be found in the appendix for the documents to be created andfor example for the business impact analysis or the IT contingency plan.

The life cycle described for IT-service continuity managementconsists of seven phases:

- Developing a policy
- Performing a business impact analysis
- Defining preventive controls
- Developing recovery strategies
- Developing IT contingency plans
- Planning testing, traning and exercises
- Updating the IT contingency plans.

The standard primarily targets government agencies of the USA, but the guide is applicable to organisations of all types and sizes.

PAS 77 / BS 25777

The publicly available specification 77:2006 “IT Service Continuity Management - Code of Practice” from the British Standards organisation [PAS77] describes the principles and methods for structuring and implementing an IT service continuity management system. This preliminary standard is available to the public but is not free of charge. PAS 77 can be viewed as a supplement to BS 25999 for the area of contingency planning for IT services. It can currently be found in the most recent version of BS 25777 “Code of practice for information and communications technology continuity”. The first draft with 38 pages was released in September, 2008 for external comments and can be obtained for a fee.

The target group of this specification is the group of persons responsible for structuring, implementing, and maintaining IT service continuity. The goal is the establishment of an IT contingency plan for the critical IT services. The corresponding safeguards and plans are intended to minimise interruptions to IT operations and guarantee fast restoration after the failure of an IT service.

ISO / IEC 24762

The ISO/IEC 24762 standard "Information technology - Security techniques - Guidelines for information and communication technology disaster recovery services" published at the beginning of 2008 is concerned with the requirements for recovery services for the information and communication technology. The standard addresses internal as well as external service providers for information and communication technology (ICT) disaster recovery (DR) services and describes the requirements for implementing, operating, monitoring, and maintaining DR services. The ICT-DR services are a part of business continuity management.

ITIL

The "IT Infrastructure Library" (ITIL) is published, updated, and refined by the Office of Government Commerce (OGC), a British government agency. The current version, ITIL V3, appeared in 2007. In the meantime, it has been accepted worldwide as a de-facto standard for the design, implementation, and management of major IT control processes. The library is actually a procedural library of best-practice publications describing methods for the planning and controlling of IT services.

IT service management is the central organisational instrument for aligning the IT with the business requirements and for controlling the IT services according to customer requirements. These service management processes form the core of ITIL.

The IT service continuity life cycle according to ITIL consists of four phases:

- Initiation of the process: specification of the policy and of the scope / applicability / IT systems
- Requirements and strategy: business impact analysis (BIA), risk analysis and continuity strategy
- Implementation: development of continuity plans, restoration plans, and test strategies
- Operative management: training and raising awareness, audits, tests, and change management.

The ITIL knowledge is available in a library containing approximately 40 publications in the English language [ITIL]. Two major components of ITIL, the management processes supporting and delivering IT services (service support and service delivery) have already been summarised and revised in a German language edition.

ISO/IEC 20000

The ISO/IEC 20000 standard "IT Service Management" is based on British standard BS 15000 and permits certification of the IT service management in an organisation. The standard consists of two parts. ISO 20000 Part 1 defines the minimum requirements that must be met for certification as well as additional requirements, policies, and recommendations. Part 2 contains best practices for structuring and operating a management system [ISO2000]. The basis for implementing the management system can be derived from the ITIL best practices. The section relevant to IT contingency planning, section 6.3 "Service continuity and availability management", specifies eight control goals that must be fulfilled to obtain certification according to ISO 20000. These goals are:

1. Business plan requirements
2. Annual reviews
3. Re-testing plans
4. Impact of changes
5. Unplanned non-availability
6. Availability of resources

7. Business needs
8. Recording tests (documentation of the examinations).

3 The business continuity management process

The business continuity management process of a company or government agency is a complex process that comprises contingency planning, business continuity and recovery , and . An efficient management system is needed to establish and maintain such a process.

3.1 Overview

A systematic procedure is necessary to design the business continuity management process. The business continuity management process consists of the following phases: initiation of business continuity management, contingency planning, implementation of the contingency planning concept, business continuity response, tests and exercises, as well as maintenance and continuous improvement of the business continuity management process.

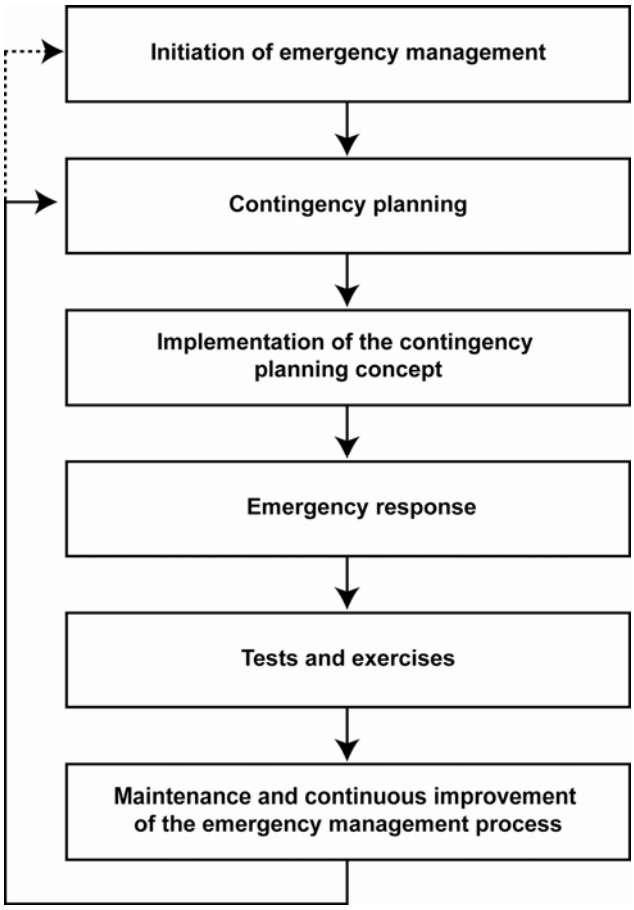


Figure 1: Business continuity management process

Before business continuity management can be established in an organisation, the general conditions must be determined. A policy for business continuity management must be created, and the policy must be initiated, developed, and released by the management. In addition, the organisational prerequisites for business continuity management must be met. To do this, the roles and responsibilities must be specified, and an adequate budget must be provided for it by the organisation's management. Successful integration of the subject of business continuity management into the existing government agency or corporate culture is decisive for the success of the business continuity management process. The employees must be integrated into the process and must be prepared for their roles through awareness-raising and training programs to accomplish this.

The information acquired through the business impact analysis (BIA) forms the foundation of the business continuity management concept. In the context of the BIA, the critical business processes of the organisation are determined and the recovery priorities are specified. In addition, the resources supporting the particular business process are determined and the minimum requirements for potential

emergency operation are identified.

A risk analysis is performed to determine the critical processes and resources. The analysis answers the question “What is threatening my processes and resources?”. If this information is already available in another management system, then a risk analysis is not necessary.

Based on the information from the BIA and risk analysis, various strategy options are worked out and the appropriate continuity strategies are selected from these options. These strategies set the framework for selecting the preventive measures, and therefore for the associated investments. Afterwards, the contingency measures are specified (contingency planning concept) and implemented. This also includes the development of a business continuity handbook that forms the foundation for responding to emergencies and is used as an aid during an emergency.

To maintain and improve the business continuity management process, tests and exercises of the methods and procedures described in the various business continuity documents, assessments of the responses to previous emergencies, as well as regular examinations are performed. The changes and optimisations determined to be required are integrated into the continuous change, improvement, and updating processes for the procedure and the plan. The repeated revision of the contingency measures and plans ensures that the business continuity management process is always appropriate.

3.2 Documentation

In the various phases of the business continuity management process, a variety of concepts, examination and test reports, and additional documents are created for business continuity management in the organisation. The decisions made can only be understood later, actions can only be repeated, and weaknesses can only be detected and avoided in the future when the decisions are adequately documented.

The quick and effective ability to handle an emergency depends primarily on the documentation available. The availability of these documents also plays a decisive role in addition to their quality and how up-to-date they are. The employees in the business continuity response team need quick access to the documents they need at any moment.

Examples of the documents to be created include the following:

- Business continuity management policy
- Contingency planning concept with the business impact analysis and risk analysis reports
- Business continuity handbook with current contact data, exercise manual, exercise plan
- Exercise concepts and records, training and awareness-raising concept
- Assessments of the responses to previous emergencies
- Audit reports and other reports
- Decision papers for management

3.2.1 Minimum requirement for the labels on documents used for business continuity management

The documents created, edited, and administered in the context of business continuity management must be informative and understandable for the particular target group. A uniform document format should be used, if possible. This improves their understandability and their handling. The documents must be labelled so that they can be found and identified quickly when needed. For this reason, the following specifications must be present at a minimum:

- Unique label (informative title)
- Author / document owner
- Function of the author
- Version number

- Date of last revision, date of next planned revision
- Release on / by
- Classification (confidential contents must be classified and labelled as such, and the documents must be stored securely)
- Authorised roles (distribution list)

The following information can also be provided as an option:

- Bibliography
- Retention period
- An overview of changes

3.2.2 Level of detail

The following principle applies in terms of the level of detail in the individual documents: "According to the goal and purpose of the document". Strategy documents such as policies should be brief and concise, but should still be informative. The documents created during the conception phase should contain detailed information so that the decisions made based on this information can be understood later on. All decisions as well as the information on which the decisions are based must be documented.

The documents needed when responding to an emergency in particular must be especially clear and easy to understand. The level of detail in the documents should allow the instructions to be understood by an outside expert. Detailed instructions for laymen are not recommended here since swift and rapid action is the goal. Simple checklists are often adequate for certain areas. Checklists provide a quick overview, help ensure that nothing is forgotten, and ensure the individual steps are followed in the correct order.

3.2.3 Change management

The currency of the information (e.g. of the contact information for reporting and escalation or of the contact persons) is of fundamental importance to business continuity management. To ensure that all documents for business continuity management are updated regularly, it is recommended to apply a change management procedure to record, release, and reproduce all changes. Clear change management instructions must be specified in writing for all documents for this purpose. The procedure should also specify how users can submit suggestions for change, how these suggestions are then evaluated and, if necessary, how to implement them. The change management process for business continuity management is to be integrated into the overall change management process of the organisation.

Update intervals should be specified for each document. Annual checks have been found to be appropriate for most of the documents. Documents containing personal and contact information should be checked at least every 3 months (although monthly checks would be even better) in co-ordination with the internal personnel administration processes.

Due to the rapid changes in the business world today, it is recommended to check the business impact analysis (BIA) every 6 months and update it, if necessary.

In addition to updating the corresponding documents during the regular checks, the documents should also be updated when the general conditions, business goals, tasks, or strategies have changed. It must be ensured that the corresponding documents are updated even after making small, yet still relevant changes. These types of changes includes, for example, personnel changes, changes to the contact data of the employees involved in business continuity management, changes to room assignments, changes to room furnishings, or IT changes, provided that these changes affect the emergency workplaces, for example.

The mechanisms triggering the change management process are to be integrated into the corresponding processes (e.g. personnel administration, building management, inventories). The

business continuity officer acts as a controlling body. The owner of a particular document is responsible for updating the document and submitting change requests for the document.

3.2.4 Documentation medium

Documents for business continuity management do not always need to be available on paper. Software tools, Internet technologies, notebooks, or even PDAs can be used for documentation purposes. They are able to store all information necessary and can be used at different locations.

It is recommended to keep copies of the business continuity handbook and all additional documents needed to respond to an emergency at hand in paper form and/or in electronic form using a simple and common format (e.g. as PDF or HTML files on a USB stick together with the corresponding viewer). The solution selected must guarantee the availability of the documents in an emergency, including in emergencies such as power failures, fires, and other risks that could make the documents unusable, destroy the data they contain, or prevent access to them. For this reason, it is recommended to keep copies at an alternative site as well. In a crisis, decisions need to be made quickly, which means there will not be time to search for the emergency notebook or for electronic documents on the server, nor will there be time to get the documents from a distant location. Even the use of software tools to administer the business continuity documents, which are seldom used or not used at all, can generate additional stress or divert the user's attention away from the actual task at hand. Instead, the processes should be simple so the user feels more secure in stressful situations.

For this reason, the documentation medium should be selected according to the need (e.g. read-only or for documentation purposes), phase (contingency planning or business continuity response phase), or subtask. Even the persons for whom the documents are intended and how familiar they are with the various media should be taken into account. For example, one person may prefer paper documents while another person may find it essential to be able to search for or filter information from electronic documents.

3.3 Security and data protection

Since the documents for business continuity management contain sensitive data on the organisation as well as personal data, information security and data protection must be guaranteed. The integrity, and especially the confidentiality of the documents must be guaranteed in addition to their availability. The various documents for business continuity management should be classified according to their confidentiality, labelled accordingly, and protected by suitable safeguards.

The authorised recipients of each document should be named in the document. Access to the documents is to be limited to those persons who need the information they contain to perform their tasks ("need to know" principle). It is therefore recommended to modularise the documents accordingly. This allows the right information to be distributed to the right recipients. An overview containing the number of the classified documents, their types (e.g. paper or CD), to whom they are distributed, as well as information on correct and complete updates, their destruction, or their return should be available in the organisation.

Very high availability requirements apply to the business continuity handbook and all additional documents needed to respond to an emergency (see also section 3.2.4), but their confidentiality should not be neglected. For example, the use of USB sticks as storage media for business continuity plansis a good choice in terms of guaranteeing quick availability, but the use of USB sticks is not recommended without additional security safeguards guaranteeing their confidentiality. Safeguards should be selected that guarantee their confidentiality but do not limit their availability in case of an emergency or a crisis. Special hardware (e.g. the use of biometric systems) or software solutions can be used for access protection or for encryption, but the risk of failure of these solutions in emergencies should be examined in advance. For example, the failure of a PKI (Public Key Infrastructure) available over the Internet or Intranet or the false rejection of an authorised user on the fingerprint reader due to moisture on the fingers in stressful situations can cause problems.

4 Initiation of the business continuity management process

The primary goal of the business continuity management process is to maintain critical business processes and keep the effects of damaging events in the organisation as low as possible. To accomplish this, strategic decisions must be made, organisational structures must be established, and safeguards must be implemented. The first step in the initiation phase is the assumption of responsibility by the government agency or management and the development of guiding principles for business continuity management.

4.1 Accepting responsibility by management

Due to the significance and wide-ranging consequences of the decisions to be made, the "business continuity management" process must be initiated, controlled, and monitored by the top-level management of the organisation. For this reason, it is important that top-level management actively examines the necessity of a business continuity management process for the organisation. Management must be provided with reasons for introducing business continuity management into the organisation.

The responsibility for business continuity management lies with the top-level management of the organisation, just like the responsibility for information security management [BSI2]. They are responsible for ensuring that all business areas operate properly and according to their purpose and that risks are detected, reduced, and their effects minimised when a damaging event occurs in the organisation.

One member of top-level management should be assigned to be the owner of the business continuity management process. This person then bears full responsibility for the business continuity management process. This member of management ensures that a business continuity management process is established in the organisation and that the specifications in the policy are met. Various legal regulations must be taken into account in this case, depending on the organisational form and industry in which it operates.

The task of setting up and maintaining a business continuity management process is usually delegated by management to a business continuity officer. However, management must be intensively involved in the contingency planning process and the business continuity response since the strategic decisions they make must ensure that no unacceptable risks are left unaccounted for and that resources are invested at the right location. Even if individual tasks performed in the framework of business continuity management are delegated to individuals or organisational units, who are then responsible for their implementation, the overall responsibility, which cannot be delegated, remains with the organisation's management.

Management must ensure that there are sufficient resources (personnel, time, and financial resources) available for business continuity management. Management is responsible for integrating the business continuity management aspects into all relevant business processes and all specialised procedures, as well as for ensuring the individual organisational units support the business continuity management process.

4.2 Conception and planning of the business continuity management process

The establishment of a business continuity management process is a project requiring planning. To estimate the time and expense required, generate schedules, and perform resource planning, the goals of the business continuity management process must be defined, the scope must be specified, the general conditions must be determined, and the strategy used to reach these goals must be specified.

4.2.1 Definition of business continuity management

The organisation's management must define what is understood by the term "business continuity management" and which tasks and competencies belong to business continuity management. Since

additional management systems such as IT management systems have generally already been set up in an organisation, all areas interfacing or overlapping with information security management, building management, quality management, or risk management should be determined.

The corresponding interfaces, responsibilities, and if necessary, rights and duties of the various disciplines should be clearly specified and documented.

4.2.2 Specification of the scope

The scope of business continuity management should be clearly specified. The scope may cover the entire organisation including all sites, only individual sites, or possibly only individual subsections. The scope should be self-contained, should not be specified in too much detail, and should completely contain the value-creating business processes and relevant specialised tasks as well as the relevant resources and necessary supporting processes. A description of the scope should also contain specifications of any restrictions and any limits of business continuity management. The most important business processes and specialised tasks contained in the scope can also be highlighted as an option.

Since the goal of business continuity management is to stabilise and ensure the ability of the organisation to survive,the entire organisation should be examined. This is the only way to guarantee effective protection of the reputation and value-creating tasks of the organisation, and therefore only way to protect the interests of the most important interest groups.

4.2.3 Legal requirements and other specifications

All significant laws, guidelines, and regulations relevant to business continuity management must be identified. To be able to identify the relevant legal requirements for the organisation, the currently applicable laws should always be checked first. There are a number of relevant field-specific specifications and relevant industry-specific standards that may need to be taken into account, if necessary. Which specifications and standards apply depends on the organisational form of the organisation, the branch in which it operates, and the type of business processes it uses. Examples of laws resulting in legal requirements for emergency management in Germany include the Sarbanes-Oxley Act, the Control and Transparency in Business Act (KonTraG), the Basel International Convergence of Capital Measurement and Capital Standards (Basel II), the Public Companies Act (AktG), the Post and Telecommunication Act (PTSG), the Stock Exchange Act (BörsG), the Occupational Safety Act (ArbSchG), the Hazardous Incident Reporting Ordinance (12. BImSchV - StörfallV), the Hazardous Substances Ordinance (GefStoffV), and the Industrial Safety and Health Ordinance (BetrSichV).

4.2.4 Objectives of and requirements for business continuity management

The organisation’s management must specify the strategic goals to be reached by establishing and operating the business continuity management process. The business continuity management strategy includes, among other aspects:

- Specification of which business goals should be protected
- Which damage scenarios are critical
- What types of business interruptions can be considered a threat to the existence of the organisation
- How willing the organisation is to take risks (appetite for risk) or how high the level of acceptance for risks is in the company or government agency
- How and at which scale should something be done about this
- What the primary goal of business continuity management is

For example, the business continuity strategy might specify that the processing of existing orders is to be emphasised and that no new business will be taken on, that all business processes should function with at least 50% of their total performance or throughput, or that the primary goal of business continuity management is to prevent damage from spreading, especially to business partners, and that

this is more important than achieving the fastest possible recovery.

The corresponding requirements for business continuity management can be derived from the business processes or specialised tasks, the general legal conditions, and especially the goals of the particular government agency or company. Even a stakeholder analysis can be helpful. In this case, the most important interest groups (referred to as the key stakeholders) having a vested interest in, and therefore an influence on the business continuity management process of the organisation, are identified regardless of whether to protect their self-interest or the interest of third parties such as society in general. Examples of possible interest groups include business owners, the employees and their families, investors, customers, and suppliers, but also insurers, supervisory agencies, industry associations, or the legislating bodies.

4.2.5 Planning principle

The time and expense required to conceive and establish a business continuity management process should not be underestimated. To ensure that neither motivation nor sense of perspective is lost, realistic goals should be set and, if necessary, the business continuity management process should be set up in several stages. It is recommended to set reasonable intermediate goals and achievable milestones. For example, in the first stage, the essential processes could be focussed on and in-depth details of each process step can be specified in another stage. Once the first level of business continuity management is reached, the BCM process can be continuously improved and brought to a higher level of maturity by improving the methods, expanding the group of business processes covered, and adding more detail to the individual process steps.

4.3 Fulfilling organisational prerequisites

Business continuity management can be divided into the areas of contingency planning and business continuity response. Contingency planning is performed pro-actively, while the business continuity response is only activated when an emergency occurs.

There are three areas of responsibility associated with business continuity management:

- The strategic area (also referred to as the Gold Team)
- The tactical area (Silver Team)
- The operative area (Bronze Team).

The strategic area of responsibility consists of the overall responsibility for the actions taken or planned in the organisation to reach the goals of the organisation and must therefore be established at the management level. The tactical area of responsibility contains the implementation of the strategic specifications for the organisational units. The operative area of responsibility implements the specifications at the strategic and tactical level.

The following figure provides an overview of the roles present in the three areas of responsibility and in the contingency planning and business continuity response phases. The descriptions found in the next two sections contain the tasks, responsibilities, competencies, and authorities of these roles.

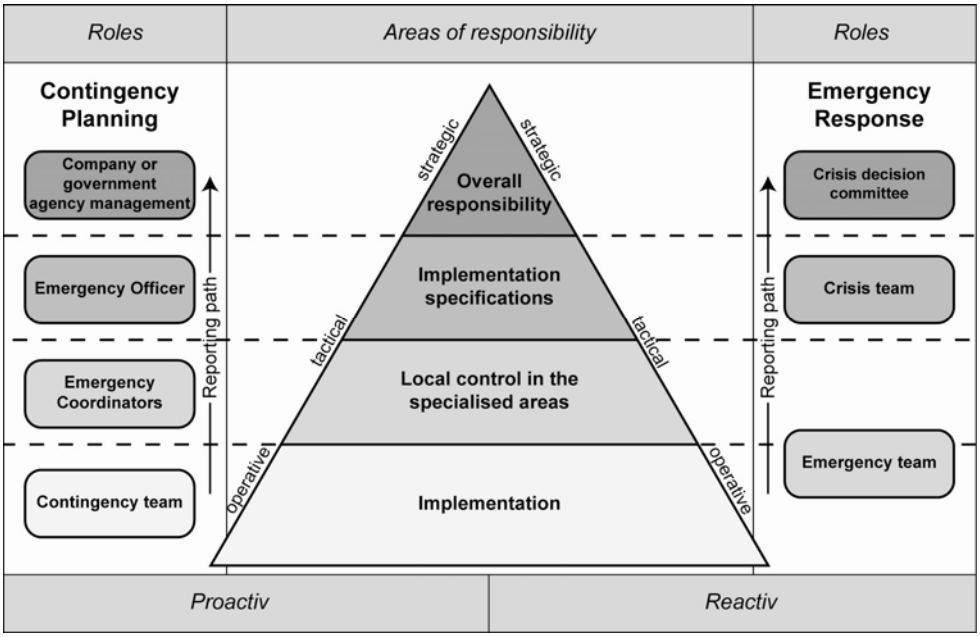


Figure 2: Roles and areas of responsibility

Not every role described needs to be present in an organisation. The roles present depend on the size of the organisation, the logical organisational structure, and the geographic distribution of the organisational units. The roles to be used and persons to be assigned to these roles must be selected suitably on a case-by-case basis. The structure selected should be documented clearly. Several roles may be assigned to a single person under the condition that the corresponding employee possesses the necessary qualifications and has enough time available to fulfil these roles. In addition, not all roles are full-time positions, and many can be assigned to existing positions as additional tasks, especially in small and medium-sized organisations.

4.3.1 Roles in the contingency organisation

Company management or head of a government agency

The company management or head of a government agency is responsible for ensuring the existence of the business continuity management throughout the entire organisation. They determine how much importance is placed on business continuity management in the organisation, determine the strategic direction when establishing the business continuity management process, and provide the necessary financial and personnel resources based on economical approaches. The organisation's management delegates the planning and co-ordination of all tasks performed in the framework of the business continuity management process to the business continuity officer, and grants the business continuity officer the corresponding authority.

The business continuity officer

The business continuity officercontrols all activities relating to contingency planning and is therefore involved in all associated tasks. He is responsible for the creation, implementation, maintenance, and support of the organisation-wide business continuity management process and of the corresponding documents and regulations. The business continuity officer co-ordinates the preparation of the resources for the groups of employees involved in contingency planning and in the response to emergencies when they occur with the agreement of the organisation's management. He co-ordinates the creation of the contingency planning concept and the business continuity handbook. He checks the implementation of the measures and safeguards, plans business continuity exercises, and co-ordinates planning with the organisation's management. He analyses the entire business continuity response process after a damaging event, is responsible for assessing the exercise results, and develops measures to eliminate defects or improve processing in co-operation with the various organisational units. He names the persons responsible for implementing the safeguards and checks their implementation. It is his responsibility to ensure the business continuity management process is

maintained and conforms to the concept. It is his responsibility to approve any changes to business continuity documents.

The business continuity officer is required to report to the organisation's management. If business continuityr co-ordinators are also employed, then the business continuityofficer initiates and heads regular committee meetings. The business continuity co-ordinators working at the different sites are co-ordinated by the business continuity officer. He has the authority to give orders to the business continuity co-ordinators in the framework of contingency planning. The business continuity officer develops procedural specifications, provides samples and templates, collects the reports from the business continuity co-ordinators, and consolidates them into an overall report for the organisation.

It must not be forgotten that the business continuity officer needs to have a qualified representative. This person should always be well-informed of the current status.

Business continuityco-ordinators

In large organisations, the business continuity officer may be supported by additional business continuity co-ordinators. Whether or not business continuity co-ordinators need to be named, and if so, how many, depends on the type and size of the particular organisation. It is recommended to appoint one business continuity co-ordinator for each large logical organisational unit. Organisational units in this case can be individual sites or regions of the organisation, or they can be formed based on the logical structure of the organisation.

A business continuity co-ordinator is understood to be a link between the organisational unit he is assigned to and the business continuity officer. He works independently on his own responsibility and performs the business continuity management activities necessary for his organisational unit. This includes performing the business impact analysis, correctly creating the business continuity plans, and consistently specifying and implementing appropriate safeguards in his organisational unit. The business continuity co-ordinator is involved in the preparation, execution, and evaluation of tests and exercises in his area. He analyses the results of regular examinations of the operability, checks if the business continuity documentation in his area is up to date, and, if necessary, works out improvements (examination of the contingency planning) for his area. He is responsible for reporting to the business continuity officer in regular committee meetings and helps the business continuity officer to prepare decision papers for the organisation's management.

Contingency team

Selected experts from the organisational units or for technical questions work temporarily with the contingency team. They provide the business continuity co-ordinators or the business continuity officer with consulting services for special subjects or implement the specifications and safeguards of the strategic contingency planning. If necessary, they also participate in the preparation, execution, and evaluation of tests and exercises.

4.3.2 Roles in the business continuity response organisation

The response to an emergency or a crisis requires a special organisational structure whose configuration differs depending on the type, scale, and seriousness of the exceptional situation. The roles in the business continuity response organisation must be clearly defined and documented together with their tasks, authorities, responsibilities, duties to inform, escalation levels, and rights. The employees assigned to these roles should be selected according to their qualifications and not according to their position in the organisation since special requirements are placed on the physical and psychological capabilities of these employees in extreme situations. Not all managers are automatically also good strategists when under pressure and, in extreme cases, can impede instead of contribute to the efforts of a crisis team. Employees in the management level are used to having complete control over a situation, thinking decisions through completely, and weighing the consequences. The experience of "losing control" in a crisis situation or needing to make decisions whose consequences to their own position and career cannot be predicted quickly and can therefore lead to side-effects ranging from a feeling of being threatened to the complete inability to take action.

For those employees assuming roles in the business continuity team, an exemption from liability

clause or a limitation of liability clause for crises should be agreed to in the employment contracts or in corresponding supplemental contracts.

Since emergency and crisis situations require a quick response and this response may be impeded by special circumstances, one or even several substitutes should be named for each role.

Crisis decision committee

The crisis decision committee is responsible for the strategic business continuity response. This committee usually consists of one or more representatives from top-level management such as members of the executive board, the management, or the agency administration in government agencies. The "thinkers" who set the strategic direction taken in a crisis and make wide-ranging decisions that go beyond the authorities granted to the crisis team leader are found in the crisis decision committee. These types of decisions include, for example, strategic decisions in crises that extend beyond the scope of business continuity management or business continuity strategies that could have long-term effects on the organisation (e.g. the complete shutdown of a process). Another task of the crisis decision committee when responding to an emergency is to initiate and maintain contact with the most important interest groups.

The actual work performed during a crisis should be left to the crisis team, though. How closely the crisis decision committee is linked to the crisis team depends on the type and size of the organisation. In some organisations, especially small organisations, there is less separation of the roles, and the crisis decision committee is represented in the crisis team by a representative from top-level management.

Crisis team

The central governing body for business continuity response is the crisis team. The term "crisis team" has become the accepted name for the business continuity response team regardless of whether the team is responding to an emergency or a crisis. The term "crisis team" is used for this reason as well in this document.

The crisis team is a body that plans, co-ordinates, and provides information and support in an emergency or a crisis. It is a special, temporary organisational structure that overrides the normal organisational structure for managing the response to an emergency and bundles authorities from all departments. The crisis team operates using a flat decision hierarchy, which means that all members of the team are in the same level of the hierarchy. It plans, co-ordinates, triggers, and monitors the response to an emergency and directs the preparation of all information and resources needed to respond to the damaging event.

The crisis team is composed of a leader, a core team, and an extended crisis team. Additional experts can also be added to the team, if necessary. The details of how a crisis team is set up depend primarily on the type, structure, and size of the organisation. The crisis team assembled for a crisis depends on the type of crisis. The following rule applies when assembling the crisis team, though: "as small as possible and as expandable as necessary".

The following tasks should be performed in every crisis team regardless of the tasks of the organisation:

- The situation must be surveyed and evaluated. All important information must be updated regularly.
- Requests to handle an emergency must be submitted to the corresponding persons responsible, and the activities needed to handle the emergency must be co-ordinated.
- Public relations and internal communication must be co-ordinated (crisis communication).
- Guidelines for the co-ordination of each measure taken must be specified

There should be at least one substitute named for each member, and two substitutes should be named for managerial positions. The recommendations for the crisis team leader specify up to four substitutes. The main requirement is that the crisis team is able to improvise when necessary.

Crisis team leader and core team

The core team is formed by the crisis team leader and a maximum of five important office managers. These people are permanent members of the team. The crisis team leader makes all decisions required in the framework of business continuity response. His wide-ranging authorities and the financial and legal framework in which he is able to operate are to be specified in advance and take effect when an emergency is declared.

When an emergency is declared, the crisis team leader decides on the size and composition of the crisis team to be summoned based on the type of event. He specifies the location from which the crisis team will operate, the crisis team meeting room, as well as the areas of the organisation affected by the crisis, since these are the only areas for which the crisis team has the authority to give orders. The normal authorities of the line organisation still apply to those organisational units not affected by the crisis. A substitute leader, generally a member of the crisis team, should be appointed in case the leader cannot be reached.

The people assigned to the core team should remain members for a long period of time to ensure experienced personnel trigger a co-ordinated reaction in an emergency. Experience has shown that the following functions should be assigned to the core team:

- The public relations policies followed by the government agency or corporate communication section
- The government agency or company security department consisting of information security as well as operational reliability (i.e. safety and security).

Depending on the type of organisation, a representative from IT operations can also be included in the core team.

Since the members of the crisis team must act calmly yet swiftly in extreme situations, need to weight the pros and cons of many difficult aspects, and must take constantly changing factors into account, the crisis team members should be selected carefully and receive the corresponding training. The leader of the crisis team should have strong leadership qualities, be able to handle and resist a high amount of stress in extreme situations, and be able to make decisions quickly when under pressure. The ability to work in a team and strong social skills are additional traits that should characterise the leader of the crisis team.

Extended crisis team

The extended crisis team consists of designated special functions or support groups that are activated for the extended crisis team depending on the type of emergency. For this reason, these extended team members are also referred to as event-specific members of the team. They could include, for example:

- IT administration / IT leader (provided that they are not already in the core team)
- Site safety personnel, e.g. the Fire Safety Engineer, environmental protection, plant safety, rescue service
- CERT leader if a CERT (Computer Emergency Response Team) is available
- Legal advisors
- Personnel representative
- Contact persons of the affected departments and business processes, e.g. of Sales, Logistics, etc.
- Contact persons from the Purchasing, Financial, Building Services, Internal Services, Organisation, and Personnel areas
- Data Protection Officer
- Industrial Security Officer

The business continuity officer is a special position providing the crisis team with support and consulting in matters relating to contingency planning. In addition to the expert representatives, the

crisis team should also be provided with a secretarial corps (crisis team assistants) for administrational support as well as a keeper of the minutes for revision-proof recording of all events and decisions.

Expert consultants in the crisis team

On the one hand, the crisis team should not contain too many people (a maximum of ten persons) to ensure fast communication and decision-making, but on the other hand, it needs to be able to handle all tasks and functions required for the particular emergency. One way of ensuring the crisis team is not too large is to resort to external specialists who are not formally members of the crisis team for support. This applies especially to crises that cannot be handled by the organisation alone, for example crises with a criminal background such as cases of extortion, kidnapping, or bomb threats.

Business continuity team

The operative part of the response to the emergency is executed by various business continuity teams. These teams are responsible for recovering and restoring business processes, applications, or systems. Classic business continuity teams are the infrastructure, IT, and business continuity teams for organisational (business units) . The business continuity teams only need to follow the orders of the crisis team when responding to an emergency.

The infrastructure team is responsible for restoring the usability of a building and the workplaces. This includes restoring power and climate control, switching networks, setting up alternate workplaces, obtaining and disposing of resources, but also rewiring the cables.

The tasks of the IT team include, among others, purchasing alternate systems, putting these systems into operation, restoring data, and eliminating malfunctions in the PBX system.

The business continuity team for organisational units are responsible for the on-site measures and for recovering the processes and specialised procedures. This includes starting work at the alternate workplaces, initiating alternate procedures or reduced operations, and finally restoring normal operations. This is done in co-operation with the business continuity teams responsible for the specialised areas. The leaders of the business continuity teams for the specialised areas (specialised area co-ordinators) are responsible for proper implementation of the business continuity plans in the corresponding units.

The business continuity team leaders must report to the crisis team at regular intervals when responding to an emergency. They collect information on-site, forward this information to the crisis team, and co-ordinate and control the on-site implementation of the measures ordered by the crisis team. If necessary, they trigger the initial measures at the damage site and act as a contact point for external support teams such as the police, rescue services, or fire department. Questions from the media should be forwarded to the crisis team or the crisis communication point.

Additional support personnel

Depending on the type of organisation and the possible damage scenarios, it may make sense to provide contingencies for psychological support for the employees, their family members, or other persons affected. Large-scale damaging events often come in conjunction with special psychological stress, especially when people are injured. If the organisation employs psychologists, then they can be prepared to provide personnel with psychological aid after large-scale damaging events or even to take care of and provide support for the crisis team with the help of additional qualifications.

Several sites

If the organisation has several sites, which may be distributed all over the world, then one of several possible models can be used to establish the organisational structure of the business continuity response:

- The entire structure, from the crisis decision committee to the business continuity teams, can be established at each site. The locations are co-ordinated by an additional (eventually international) decision committee.
- Every site has its own local crisis team and local business continuity teams. The sites are co-

ordinated by the central crisis decision committee.

- The decision committee as well as the crisis team operate centrally; only the operative business continuity teams are located at the site.

The model suitable for an organisation to handle a crisis spanning several sites must be chosen on a case-by-case basis, and the choice depends primarily on the general organisational structure, the size of each site, the dependencies between the sites, and the geographic distribution of the sites.

4.3.3 Interaction with the information security management

In addition to the roles in the contingency planning and business continuity response, there are also roles and areas of responsibility for information security management in every organisation. In addition to abusiness continuity officer, each organisation should also have an IT Security Officer who is responsible for protecting all aspects relating to information security in the organisation.

Since some of the areas of responsibility in the business continuity management and information security management concepts overlap, the extent to which the BCM officer can also assume the role of the IT Security Officer or the IT Security Officer can assume one of the business continuity management roles must be clarified. These roles are not necessarily mutually exclusive; the deciding factor is the type and nature of the organisation, the intensity of IT use in the business processes, and the type of security management implemented. The more dependent the business processes are on the IT, the more the two disciplines overlap. The security management system established must take a holistic and process-oriented approach and should not focus only on IT. These are the only conditions under which it makes sense to have the same person assume the roles of the IT Security Officer and the business continuity officer.

There are some aspects that need to be clarified in advance:

- The interfaces between the various roles should be clearly defined and documented. In addition, direct reporting paths to superiors should be available on all sides. Ideally, these reporting paths should be identical so that all report to the same person in top-level management.
- Consideration should be given to informing the internal auditing department when highly contested subjects arise.
- It must be ensured that persons assuming more than one role are adequately qualified and are provided with enough resources to perform their tasks.

4.4 Creation of a policy for business continuity management

The value placed on business continuity management in the organisation and the strategic direction should be summarised in a policy for business continuity management. This policy defines the framework for the conception, establishment, and maintenance of the business continuity management system.

In just a few pages, the policy describes why a business continuity management system should be set up and what the goals of business continuity management are.

The policy is to be created by a correspondingly qualified team. The business continuity officer is active in the process as a co-ordinator. Since the business continuity management policy is the central strategy paper, it should be designed so that all affected organisational units can identify with its contents. For this reason, it makes sense to allow as many specialised areas as possible as well as the organisation’s management to be involved in its creation so it will be accepted by all. It is recommended as well to involve representatives from the specialised areas, the personnel representative, and representatives from the company or government agency security staff (information security and operational reliability), the internal auditing department, risk management, corporate or government communication, the information technology department, or the legal department. The areas from which representatives should be selected can and must be decided individually by each organisation.

Contents of the business continuity management policy

A business continuity management policy should be brief, concise, and should cover the following aspects at a minimum:

- A definition of business continuity management
- The value placed on business continuity management by the organisation
- The objectives
- The core statements of the business continuity strategy
- The scope
- The procedural model or standard (for example BSI Standard 100-4) on which business continuity management is based
- The business continuity management structure with the most important roles and their responsibilities
- The duties of the organisation's management to optimise the business continuity management procedures through regular examinations, tests, and exercises
- The relevant laws, policies, and regulations that need to be followed
- The acceptance of responsibility by the organisation's management (which also needs to be documented by explicitly approving the document with a signature

Optionally, general statements relating to supervising and checking the success of the business continuity management process can be provided.

Releasing the policy

The business continuity management policy must be published in the organisation and made available to all employees and potential interest groups. The persons participating in the business continuity management process in particular should be informed of the policy and confirm in writing that they have read the policy.

Updating the policy

The policy is to be updated at regular intervals and when there are changes in the general conditions, business goals, tasks, or strategies. The business continuity officer is responsible for co-ordinating the execution of these tasks. The updates should be performed together with the management. The updated policy must be released by the organisation's management per signature and then published.

4.5 Providing resources

The structure and the operation of a business continuity management process requires financial, personnel, and scheduling resources. This fact should be taken into account when specifying the business continuity strategy and the safeguards for protecting the critical business processes. The level of security strived for should be economically feasible. The amount of resources needed for business continuity management depends primarily on the size and type of organisation and the type of business it does, but also on the location, the environment, the customers, the technologies used, and the willingness of the organisation to take risks (appetite for risk).

4.5.1 Cost-efficient business continuity strategy

For a cost-efficient business continuity strategy, the investment costs should be weighed against the benefits obtained, but also against the necessity for security. Benefits include the avoidance of the costs incurred when a threat arises and the costs incurred due to the failure or malfunction of critical business processes. This means that the same problems arising when trying to convince management of the necessity for information security management also arise in the case of business continuity management.

The costs avoided consist of direct costs as well as indirect costs. Direct costs include costs such as lost sales or orders, production shutdowns, penalties due to breaches of contract or non-compliance with regulations, and the cost of restoring the systems. There is a wide range of indirect costs. These costs include, for example, reputation damage and loss of trust. These losses can then lead to a loss of customers or a weaker market position, and in turn to higher investments to acquire new customers or to regain trust.

Since only very rough estimates of the costs and benefits of establishing a business continuity management process are available at the start of the project, it is recommended to examine the business continuity strategy initially specified in the course of the project, but also to examine the business continuity management process during live operations. Only after performing these examinations is it possible to obtain more detailed estimates of the costs of failures and of investment. If the demands placed on business continuity management are too high for the financial capabilities available, then the business continuity strategy should be revised.

4.5.2 Resources for the business continuity response organisation

The operation, and especially the structure, of a business continuity management system requires personnel resources. When establishing a business continuity management system, the business continuity officer and, if necessary, the business continuity co-ordinators, should be released from their regular tasks to enable fast implementation. Depending on the size of organisation, these employees can perform their tasks in business continuity management in addition to their original job. Very few organisations have the ability to provide full-time positions for the business continuity co-ordinators or the members of the contingency team.

Resources are not only needed for contingency planning. The time required for the employees assigned to respond to an emergency should not be underestimated. Hopefully, less time will be spent in these roles during an actual crisis, and more time will be spent on actively engaging in the necessary tests and exercises. Depending on the scope of the exercises necessary for the organisation, it may be necessary to release the employees temporarily from their original jobs.

Adequate resources should also be provided so that the effectiveness and suitability of the contingency measures and of the business continuity management process can be tested regularly and systematically. During the examination, the efficiency of resource utilisation should be compared to the benefits gained. If it is determined that certain measures generate uneconomically high costs, then alternative measures should be investigated or the continuity strategy (see section 5.4), the requirements from the business impact analysis, or even the business continuity strategy itself should be re-examined. The integration and implementation of suggestions for improvement as well as the elimination of all defects detected should also be taken into account when planning the personnel resources.

In practice, the persons responsible in the organisation for business continuity management often lack the time to analyse all relevant influence factors and general conditions (e.g. legal requirements or technical issues). Sometimes they also lack the necessary basic expertise at the beginning of the project. In this case, it may make sense to use external experts. The use of external experts should be communicated and documented by the business continuity officer so that management can provide the necessary resources.

4.5.3 Resources for preventive measures and their operation

Preventive measures include organisational, infrastructural, and technical measures in addition to personnel measures. A reasonable combination of suitable measures should be selected. In many cases, investments in personnel resources and organisational regulations are just as effective and efficient as investments in technology. Technology alone does not solve any problems, which is why technical and infrastructural measures should always be integrated into a suitable organisational framework. However, the targeted use of technical measures is also decisive, and the correct selection, administration, and regular examination and testing for proper function of such technology is also of prime importance. An investment in a technology that fails in an emergency is a wasted investment.

4.5.4 Co-operation with other management systems

It will become clear in the following chapters that some areas of business continuity management overlap with other management systems such as the information security management or the (IT) risk management. Sensible integration of the business continuity management system into the existing structure; good company or government communication between the disciplines and the business areas; the open, constructive exchange of the information needed; and a clear division of tasks are the primary factors in the success of the management system and in keeping the costs low. Through directed and prompt co-operation with the overlapping management systems, it is possible to utilise synergy effects and save financial, personnel, and scheduling resources.

4.6 Including all employees

To successfully introduce and maintain a business continuity management system, this management system, like all other organisation-wide management systems, must be solidly anchored in the government agency or corporate culture. Business continuity management affects all employees without any exceptions, even if it affects them in different ways. Every individual can contribute to the success of the business continuity management system and prevent damage by acting responsibly and being aware of the risks. Awareness-raising and training programs for the employees are a necessary prerequisite for this. The first step is the publication of the business continuity management policy. Even the work climate, commonality of values, and the motivation of the employees have a decisive influence on the robustness of business processes, and therefore of the organisation.

4.6.1 Training and raising awareness

Raising the awareness of the employees in terms of business continuity management is given a high priority in the BCM life cycle. An awareness-raising and training program as well as topic-related presentations should be employed to ensure that all employees in the organisation know an business continuity management system exists, the reasons for having the system, how they can contribute to the successful implementation of the business continuity management process, how they can integrate the process into their workday, and how they should respond in an emergency. Since the employees have different needs in terms of raising their awareness, the program should be oriented towards specific target groups and be designed to meet all needs. A suitable depth and form of the training and awareness-raising program is to be selected based on these needs.

The employees performing the contingency planning as well as those responding to an emergency must be prepared and qualified specifically for their tasks through training. To create a training concept, the type of training needed has to be determined and documented first. In the next step, the subjects and contents (for example BIA, risk analysis, communication with media, training the members of the business continuity response teams) must be identified. The type of training used should be specified and documented. Types of training include, for example:

- Computer-based or Internet-based learning
- Individual or group training using internal or external personnel
- Seminars

The government agency or corporate communication paths already in use, for example management conferences, regular meetings, introductory seminars for new employees, presentations by organisational units, employee newspapers, posters, or newsletters should be used to raise awareness. It makes sense in this regard to use a co-ordinated approach and utilise the awareness-raising measures implemented by security or risk management.

The leaders of the organisational units should actively support and participate in the training of their employees and should also release them from their daily tasks for such training measures. After completion of an awareness-raising and training program, it should be examined if the information presented in the program was correspondingly understood by the employees. The implementation and progress of the training and awareness-raising program are to be documented accordingly. Proof of the fact that the training programs were held is to be saved accordingly. It is also recommended to

evaluate the efficiency of the awareness-raising and training programs held. The organisation's management is to be informed annually of the status of the measures.

4.6.2 Integration, risk communication, and early detection

To increase the resilience of an organisation and to be prepared for an emergency, it is not only necessary to raise awareness of the employees regularly, but also tocreate suitable organisational structures so that business continuity management can be actively integrated into daily activities. To do this, the contact persons and people responsible for this topic must be specified, and the employees must be informed accordingly.

The employees are to be integrated into a regular flow of information regarding risks, incidents, and effects. When any employee detects a potential risk to business continuity during daily operations or even just suspects such a risk is present, the employee should know how to respond and who he can report to regarding the risk. This pro-active communication of potential risks is also referred to as risk communication in the field of business continuity management. Risk communication can contribute to the early detection of risks and the initiation of countermeasures to ward off an emergency or quickly contain it.

5 Conception

A wide variety of preparatory work must be done before developing a contingency concept consisting of a contingency planning concept (see section 5.5) and an business continuity handbook (see section 7.4). The goals of this work are to understand the company or government agency and its "business", identify the availability requirements of the business processes, detect vulnerabilities, establish countermeasures, and prepare for any remaining risks by implementing a functioning BCM response system.

A business impact analysis supplies the necessary information on the critical business processes and resources. A risk analysis supplies the necessary information on existing risks against which the organisation should implement safeguards. The development of continuity strategy options points out possible alternatives for implementation. The suitable continuity strategies are selected by management. These strategies then form the framework for creating the contingency concept and contingency plan.

5.1 The business impact analysis

The central task of a business impact analysis is to understand which business processes are important to maintaining the business operations, and therefore of the organisation, and what possible effects a failure can have. These "critical" business processes are provided with special protection in the framework of business continuity management, and precautions are taken in case of a crisis.

"Critical" in the sense of business continuity management means "time-critical", which means that this process must be restored to operation faster because otherwise a high amount of damage to the organisation can be expected. The high damage resulting can consist of financial losses, violations of laws or contracts, reputation damage, or other damage scenarios. A business process determined to be "uncritical" by the BIA does not mean that this process is not important to the organisation, but that its restoration is assigned a lower priority.

To identify the "critical" business processes and develop suitable strategies and preventive measures for damaging events, the effects of malfunctions, interruptions, or even the loss of business processes in the organisation must be determined first. To do this, the most important products and services provided by the organisation and the corresponding processes must be identified. The critical business processes generally contribute to providing the most important services and generating the products, but a limited view of these processes alone should be avoided .

In this phase of the business continuity management process, the question of what caused an emergency is not of interest yet; only the consequences expected by the organisation are of interest. To determine these consequences, a business impact analysis (BIA) is performed. A BIA is a procedure used to specify the recovery points of the business processes, assign recovery priorities, and therefore determine the criticality of the business processes, as well as to identify the necessary resources.

There are many methods and ways of performing a business impact analysis. There is no one "true" way or "best practice". How the needed results will be obtained can be decided by the organisation itself. This standard presents a method that is based on the protection requirements determination according to BSI Standard 100-2 for structuring an information security management system according to IT-Grundschutz. The methodologies of the business impact analysis and the protection requirements determination according to BSI Standard 100-2 have some common elements so that synergy effects can be utilised and time and expense can be saved when these two disciplines co-operate, or at least exchange all information they have available. The common elements and how to extend the protection requirements determination to obtain the results of a BIA are explained in the following.

5.1.1 Overview

A business impact analysis can be divided into the following steps (see Figure 3):

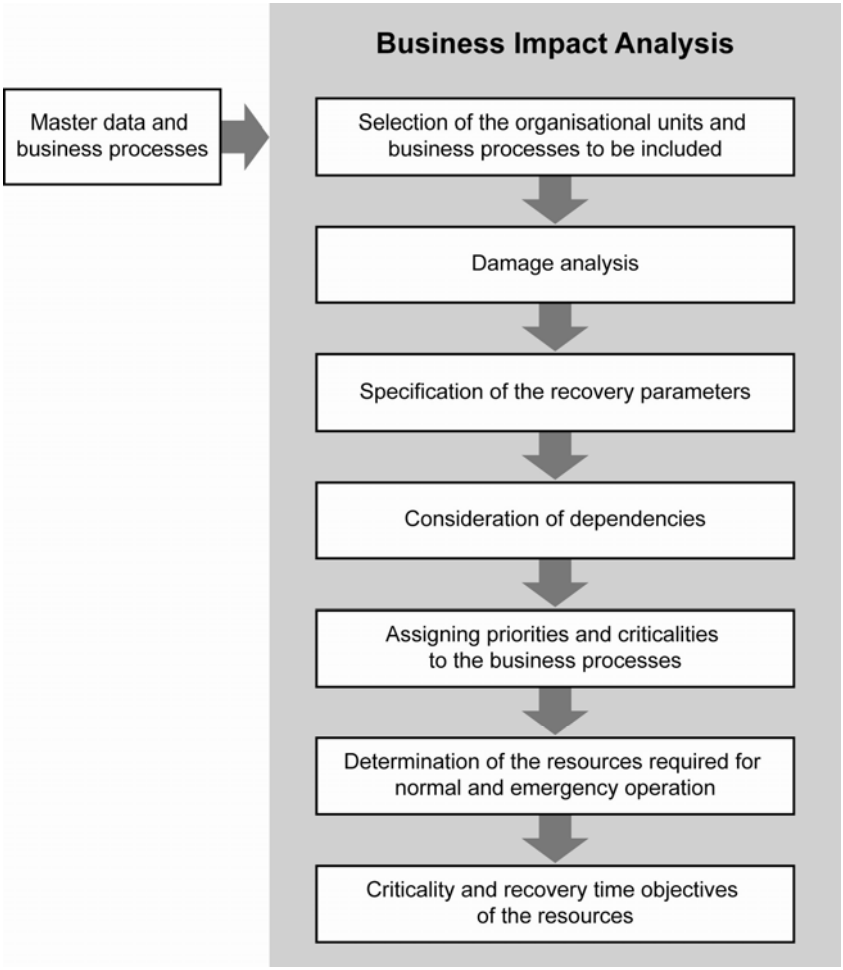


Figure 3: Overview of a business impact analysis

Step 0: Master data and business processes

To perform a BIA, an overview of all relevant business processes in the company or all specialised tasks of the government agency is needed together with information on the corresponding contact persons and persons responsible for the processes. This overview should contain the list of processes, which business goals they are assigned to, and the dependencies between the individual processes. The business goals of a government agency are usually derived from the tasks they are assigned to perform. If no current process overview is available, then this overview must be created or updated in the course of preparing for the BIA. In addition, the master data of the organisation such as the corporate structure or locations should also be provided.

Step 1: Selection of the organisational units and business processes to be integrated

If it is obvious, considering the specified scope of business continuity management, that some organisational units or business processes are not very important for reaching the business goals and are not important for the value-creating processes of the organisation, then these units or processes do not have to be examined any further.

Step 2: Damage analysis

A damage analysis examines the damage that could be done to the organisation when individual business processes fail. In this case, not only is the amount of damage important, but the chronological sequence of the damaging events is of particular interest. The general conditions for performing the damage analysis (damage categories and damage scenarios), the evaluation periods, and the strategy for handling special time periods in which the availability requirement of a process will need to deviate from its average availability must be specified. Afterwards, the damage resulting from a failure is evaluated for each individual process and in each evaluation period.

Step 3: Specification of the recovery parameters

Based on the chronological sequence of damaging events and the amount of damage expected, the maximum tolerable period of disruption, the recovery time objective, and the recovery level for each business process is specified. The results are then collected at a central location and consolidated.

Step 4: Taking dependencies into account

Since the recovery parameters were specified individually for each process, the parameters should be fine-tuned after specification. When fine-tuning, the process dependencies and strategic business goals are taken into account, and any parameters needing correction are adjusted accordingly.

Step 5: Prioritisation and criticality of the business processes

Based on the data available for recovery and the resulting damage, the order in which the business processes will be recovered and the criticality of each process is specified. To do this, the criticality categories and their boundaries must be defined.

Step 6: Determining which resources are required for normal and emergency operation

To be able to develop continuity strategies and specify preventive measures, it is necessary to identify the resources used by the critical business processes. The types of resources and the capacity required for normal operation and for emergency operation must be determined. The information for each resource must also include specification of the maximum allowable loss of data, which is reflected in the so-called recovery point objective (RPO).

Step 7: Criticalities and recovery time objectives of the resources

In the last step of the BIA, the recovery and restoration time objectives of the resources used by the critical processes as well as their criticalities are determined.

5.1.2 Performing a business impact analysis

In the following section, we provide information on how to perform each of the steps of a BIA in detail. The information required can be determined using questionnaires, workshops, or individual interviews. It makes sense to select a combination of this methods since they each have their own various advantages and disadvantages, and sometimes complement each other. For example, questionnaires, whether in paper form or software-based, can only be formulated generally and must apply to all specialised areas and business processes. Workshops, which can reach a large number of people, are suitable for introducing the subject of business continuity management and informing the employees why certain steps need to be performed as well as what the goals of each step are. Individual interviews with the leaders of the specialised areas, the persons responsible for each process, or other personnel able to provide such information can take time, but they can provide specific information since misunderstandings can be avoided and eliminated by posing the questions correctly using suitable questioning techniques and the essential information can be provided in the desired form.

The interview partners selected when performing the BIA depend on the particular process step, but especially on the structure of the organisation.

The support of the organisation’s management is particularly important when performing a BIA. Since extensive co-operation is required from the business areas, the organisational units, and at the resource level (e.g. IT administration), it must be ensured that top-level management supports the BIA process and informs everyone in the organisation of why it is important to perform a BIA.

5.1.2.1 Master data and business processes

A prerequisite for the BIA is comprehensive knowledge of the business model and tasks of the organisation as well as the organisation’s structure. This includes knowledge of the business processes and specialised tasks as well as the master data of the organisation. The master data includes, for example, information on its legal form, its industries, its organisational structure, its sites, or its

suppliers. Specialised tasks are business processes in government agencies. When the term business process is used alone in the following, it also implicitly refers to the specialised tasks. This is done to improve the readability of the document.

Every organisation should have a complete, current, and well-documented overview of their main processes. If an up-to-date overview is not available, then one must be created or the existing one updated. Note, though, that this is not originally a task of business continuity management.

There are no clear and generally applicable specifications regarding what is understood to be a business process (see Figure 4). This document is based on the following idea: a value-added chain comprises the entire path of a product or service from the manufacturer to the consumer and can include several organisations. A value chain is understood to be those parts of the value-added chain that are located within the organisation. It consists of several interdependent business processes (process chain), generally starting with the order and continuing through to delivery and invoicing. A business process can be viewed as a series of (sub)processes in which actions are performed and decisions are made. Every subprocess is in turn a business process. A process generally needs input, which is delivered by other business processes. A process supplies results (output), for example in the form of products, information, or services, which can then be handled by subsequent processes. The inputs and outputs represent the connections between the processes. To make performing a BIA easier, it helps to specify the business processes so that they are located entirely within a single organisational unit (if possible), and therefore within a single area of responsibility and authority.

Business processes are classified by type into core processes and supporting processes. Core processes are processes that contribute directly to achieving one or more business goals. Core processes can be further divided into the categories of strategic processes, which are used by the organisation to make strategic decisions, and operative processes, which are part of the operative business. The operative business for a government agency could be, for example, fulfilling the governmental tasks assigned to it, providing services, or even manufacturing a product.

Supporting processes do not contribute directly to reaching the business goals, but can be very important indirectly and therefore still play a critical role since they are needed to maintain the core processes. Classic examples of supporting processes include personnel management and IT administration.

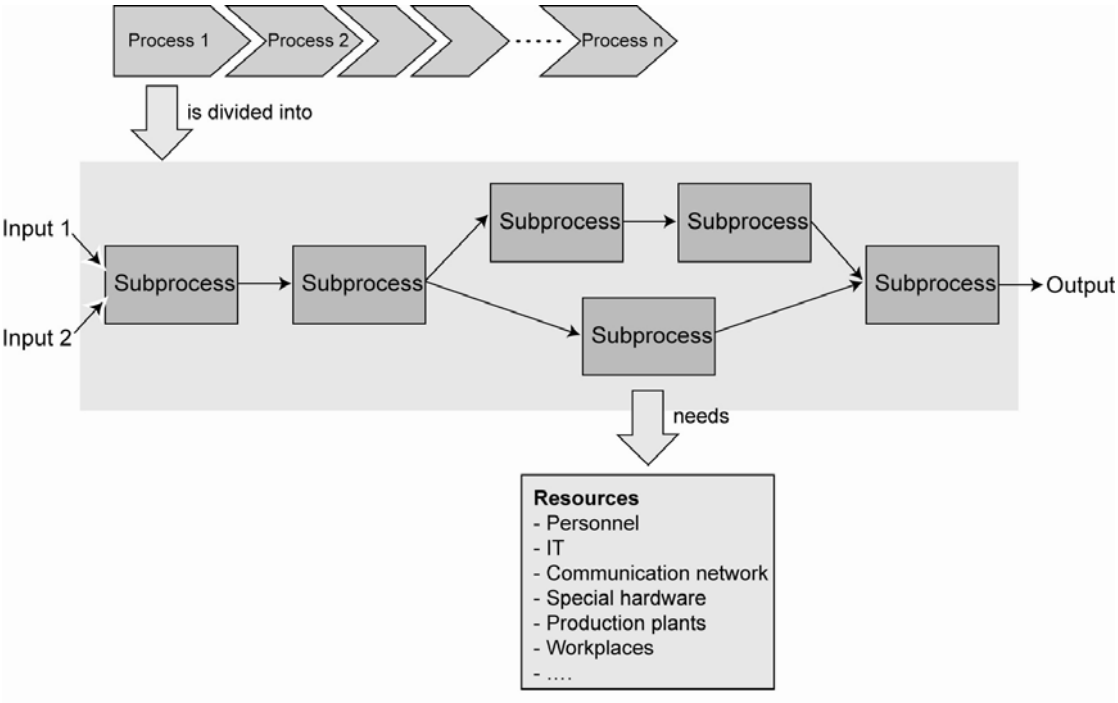


Figure 4: Business processes

The creation of the process overview requires, on the one hand, an overall perspective of the

procedures in the organisation as well as knowledge of each of the tasks. One method used to ensure all core processes are determined is to examine the value chains starting with the order and continuing to delivery and invoicing. It is recommended to delegate the task of determining the core processes to the particular organisational units. The individual organisational units then develop the business processes for their areas. The survey can be done by the leader of the organisational unit, by a person appointed to be responsible for the survey, or by the business continuity co-ordinator responsible for this organisational unit. The business continuity co-ordinator should possess the necessary knowledge relating to the business processes and contact persons since he needs this information to perform his tasks in business continuity management.

If the business process survey is performed in the framework of contingency planning, then the business continuity officer must monitor this task as a source of information, as a co-ordinator, and as a controller. To obtain comparable results, he should specify the method to be used for the survey, the method used to present the results, the level of detail to be provided for the processes determined, as well as classes and uniform general conditions. These are to be used by the organisational units when determining the core processes. The business continuity officer should consult with the corresponding personnel early in each of the organisational units to detect major differences in the way the processes are presented and initiate the corresponding countermeasures. He collects the individual results and consolidates them in co-operation with management. The result should be a process landscape that lists the processes and points out the various dependencies between the individual business processes. This includes the process or value chains as well as the dependencies of the supporting business processes.

If individual business processes that are part of a value chain in the organisation were outsourced, then these processes should also be added to the overview and labelled accordingly. The most important aspect in this regard is the illustration of the connections to the internal business processes and their interdependencies.

When specifying the level of detail to be determined for the processes, a happy medium between a highly generalised view of the processes and a highly detailed view should be selected. Placing too many processes in one business process can result in an overly general process. A too detailed view results in the need to examine an unmanageably large number of processes. Practical experience has shown that when creating the BIA, the level of detail selected when examining the individual business processes should be detailed enough to enable the formulation of specific requirements for certain applications, but also not so detailed that a complete business process analysis is necessary. A general rule of thumb is that the result of the process survey for business continuity management in an organisational unit should contain between a minimum of 5 and a maximum of 15 processes. This has proven useful in practice, but the resulting number of processes can be outside of this range depending on the organisation and the task.

The following information at a minimum must be determined for each business (sub)process:

- A unique identifier for the process
- A short description
- The input needed
- The output
- The subprocesses (if divided into subprocesses)
- The links to other internal and outsourced business processes (predecessor and successor processes) and the dependencies on supporting processes such as IT services
- The degree of dependency of the business processes (see section 5.1.2.5)
- The contact person or person responsible for the process.

Support for the process survey can be obtained using suitable business process modelling tools.

5.1.2.2 Selection of the organisational units and business processes to be integrated

If it is obvious within the specified scope of business continuity management that some organisational units or business processes are not very critical to the organisation, then these units or processes do not have to be examined any further. This can reduce the time and expense of such a survey to a certain degree. In this case, though, it must be noted that the level of dependency between some processes is not always obvious or is sometimes underestimated. The same applies to outsourced processes. Outsourced processes may only be excluded from the survey when they have been clearly classified as non-critical processes.

If there are organisational units that have been assigned a low priority for strategic reasons by the organisation's management, then the scope of the business processes to be surveyed can be further restricted, if necessary. This decision can only be made by the top-level management, though.

If the scope of the survey is restricted in this manner, then understandable reasons must be provided in writing for why each business processes or organisational unit was excluded. This restriction must be approved by the organisation's management and confirmed by signature. The reasons for exclusion from the survey should be intensively examined the next time the BIA is updated to check if the argumentation provided makes sense and has proven to be correct.

5.1.2.3 Damage analysis

A damage analysis is used to examine the potential damage to an organisation caused by the failure of individual business processes. In this case, not only is the amount of damage of interest, but also (and especially) its chronological development. A variety of general parameters must be specified for the damage analysis. These parameters include the damage categories, damage scenarios, evaluation periods to be examined, and the strategy for handling special time periods.

A. Specification of the damage categories and damage scenarios

The damage resulting from the failure of a process is comprised of the direct damage (e.g. lost profits or losses due to legal consequences) and indirect damages (e.g. lost orders, loss of market share, or loss of image). Since there are only few well-founded figures for the damage classes mentioned, it does not make sense to calculate the damages quantitatively, but to classify the damages qualitatively into damage categories. Every organisation must specify for themselves what each of the damage categories means. Organisations usually use three to five categories. The example in this document shows a division into four categories (see Table 1). The damage categories are comparable to the protection requirements categories for the protection requirements determination according to IT-Grundschutz [BSI2]. Table 1 shows a comparison of the damage categories and the protection requirements categories.

Damage categories		**Protection requirements categories**	
Category	Explanation	Category	Explanation
"low"	Failure has a minor, barely noticeable effect.		
"normal"	Failure has noticeable effects.	"normal"	The effects of the damage are limited and manageable.
"high"	Failure has serious effects.	"high"	The effects of damage can be considerable.
"very high"	Failure or impairment leads to effects that threaten the existence of the organisation.	"very high"	The effects of the damage can reach a catastrophic level that threatens the existence of the organisation.

Table 1 : Damage categories and protection requirements categories

The definition and specification of the limits of each damage category can be based in principle on the direct monetary damage, but it makes more sense to allow other damage scenarios to flow into the evaluation. The immaterial or indirect financial damage can actually be higher than the direct financial damage depending on the industry and organisation. A subset of the damage scenarios obtained from the determination of the protection requirements have proven themselves in practical applications:

- Financial consequences
- Impaired ability to perform tasks
- Violations of laws, regulations and contracts
- Negative internal and external effects (image damage)
- Personal injury

Other examples of optional damage scenarios include:

- A lack of management or control information
- A drop in the level of motivation of the employees

An organisation must specify which damage scenarios should be used, possibly together with their priorities. For most companies, the financial effect is the most important criterion, but in some industries such as banking or insurance, the damage to their image also plays a very important role. For government agencies, the ability to perform their tasks is given the highest priority, followed by damage to their image. Any number of damage scenarios can be selected, or new number of damage can be specified.

To be able to define the boundaries of the damage categories, the boundaries must be specified individually by the organisation itself based on the damage scenarios (see Table 2). If the BIA is performed together with the protection requirements determination and the subset of damage scenarios suggested is used, then it makes sense to use the specifications from the protection requirements determination to define the damage categories.

This also means there is less work to do. Table 2 shows one possibility for the suggested scenarios and categories, although these must be customised accordingly for each organisation.

Damage category “low”	
Financial consequences	No appreciable consequences (e.g. the loss is less than 5% of the annual sales)
Impaired ability to perform tasks	No appreciable effects
Violations of laws, etc.	No appreciable effects
Negative internal or external effects	No appreciable effects
Damage category “normal”	
Financial consequences	The financial damage remains tolerable to the organisation (e.g. loss of less than 5-20% of the annual sales)
Impaired ability to perform tasks	Impairment is tolerated by the employees / other tasks can be given preference / post-event tasks do not noticeably impair the ability of the organisation to perform its tasks / other organisational units or contract partners experience only minimal work disruptions

Violations of laws, etc.	Violations of laws and regulations with minor consequences / violations are only noticed internally
Negative internal or external effects	Only individual malfunctions or failures are noticed and customers and business partners estimate them to be insignificant / customers and business partners do not draw any consequences / the basic trust in the organisation is not affected / no noticeable loss of market share
Damage category "high"	
Financial consequences	The resulting damage leads to substantial financial losses, but does not threaten the existence of the organisation (e.g. loss of less than 20-30% of annual sales)
Impaired ability to perform tasks	Unacceptable interruptions or limitations / reduction in the work quality / missed deadlines are noticed by outsiders / work backlogs cannot be reduced during normal working hours / the work of other organisational units or contract partners is significantly disrupted, which means there are also backlogs to be reduced there / amounts of conventional penalties are still within an acceptable framework
Violations of laws, etc.	Violations of laws and regulations with acceptable consequences / violations are also noticed by persons outside the organisation
Negative internal or external effects	Malfunctions or failures are clearly noticed by customers and business partners as well as in the industry / the image of and trust in the organisation is tarnished in the eyes of some customers and business partners / the loss of image and trust can only be regained in conjunction with a great deal of time and expense / individual customers and business partners draw consequences and terminate the business relationship / noticeable loss of market share / losses can only be regained with some time and expense
Damage category "very high"	
Financial consequences	The financial damage threatens the existence of the organisation (e.g. if the loss exceeds 30% of annual sales)
Impaired ability to perform tasks	Seriously impaired ability to perform tasks / backlogs can only be reduced with external help or cannot be reduced / delayed and faulty results are clearly noticed by outsiders / serious reduction in the service quality / the work of other organisational units or contract partners is impossible / high liability claims, conventional penalties
Violations of laws, etc.	Violations of laws with consequences for business operations and individual employees
Negative internal or external effects	A significant number of customers and business partners draw consequences from the incidents / the image of, trust in, and reliability of the organisation are seriously impaired and are basically cast in doubt / loss of image and trust is difficult or impossible to compensate for / strong loss of market share / losses are difficult or impossible to compensate for

Table 2: Example of boundary specifications for the damage categories

After specifying which damage scenarios can be used in the evaluation, the individual scenarios are not weighted yet in the in terms of their significance to the organisation. Weighting the damage scenarios makes sense when the significance of the "Financial consequences", "Impaired ability to perform tasks", "Violations of laws and contracts", "Danger to life and limb" and "Negative internal or external effects" damage scenarios differ from the organisation's point of view, and the organisation wishes to place more emphasis on one or more scenarios.

B. Specification of the evaluation periods to be examined

A BIA, in contrast to a protection requirements determination, not only evaluates which effects the failure of a process will have on the organisation, but also how the damage develops chronologically. To do this, it is necessary to specify evaluation periods. For each evaluation period, the damage in case of a failure of the particular business process is evaluated by specifying the damage category.

The number of evaluation periods as well as the length of each period should be selected individually by the organisation since they depend highly on the existing conditions. The conditions are, for example, the types of services offered, the variety of business processes, the types of products manufactured, or just the industry together with the applicable legal regulations. For example, the individual evaluation periods selected for a bank are probably very short, while organisations with a less time-critical business model will select periods that are much longer. The recovery classes of the business processes (see section 5.1.2.6) can be used as an aid to help specify the number and duration of the evaluation periods provided that the recovery classes have been defined or will have been defined by this time.

In practice, division into four to ten evaluation periods has proven useful for organisations with average requirements in terms of the availability. The following table shows various examples of how to divide up the evaluation periods. The times specified are understood to mean "up to ... hours".

	Evaluation periods (96 hours = 4 days, 168 hours = 1 week, 720 hours = 1 month)									
Time period	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Example 1	24	72	240	720						
Example 2	8	24	48	72	168	720				
Example 3	1	2	4	8	24	48	96	168	240	720

Table 3: Examples of evaluation periods

It may make sense to add one more evaluation periods, for example a period of "> 3 months", to cover all cases in which the infrastructure has been seriously damaged, the location will not available any more in the foreseeable future, and no plans were made regarding alternate sites. If there are no alternate sites available and no preventive measures have been taken in this regard, then the restoration measures, starting with the search for a suitable location, will take a significant amount of time.

C. Special time periods and events

Sometimes the availability requirements of business processes will fluctuate greatly when viewed over time frames spanning one day, one month, or one year. Examples of such periods include specific time intervals (e.g. a daily cut-off time (tax times or other special times) in banks, copy deadlines for the advertisements in a weekly newspaper, the end of the year for an annual balance sheets, the months before Christmas for an online shop, a certain day of the week for the publisher of a weekly magazine), or certain events (e.g. an interest rate increase for a bank or a break during the transmission

of a soccer game for a waterworks).

Every organisation must make and document the corresponding strategic decisions regarding how to handle these seasonal or event-based influences on the availability requirements when performing the damage analysis. For these reasons and for use as a basis for the strategic decisions, these time periods and the possible events should be determined together with their probabilities of occurrence and a rough estimate of the variability of the availability requirements for the corresponding processes. Special time periods can be shown graphically in a calendar (see Figure 5). Special events whose time of occurrence cannot be specified must also be listed.

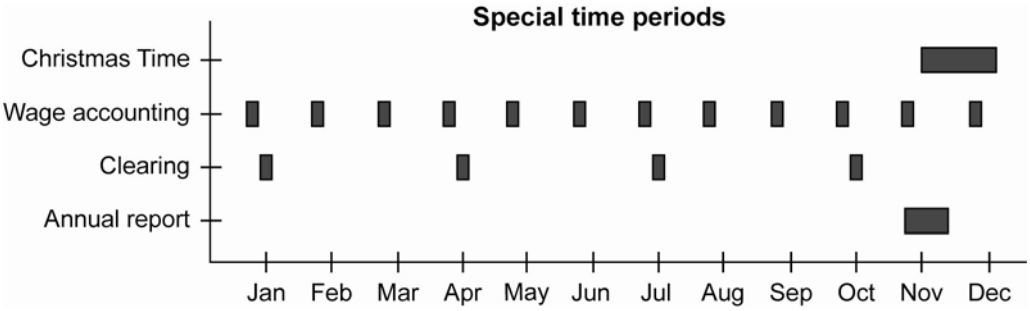


Figure 5: Special time periods

The mere knowledge of the special time periods and special events can be important information when making decisions when responding to an emergency and when planning and specifying the times for tests and exercises. Tests and exercises should not in be scheduled in those time periods where the availability requirements are higher.

Possible variations of the strategy for handling special time periods and events include the following:

- The damage analysis is based on the worst-case scenario, meaning the scenario with the highest availability requirement for the particular business process in to the special time periods and events is applied to the entire time period.
- In the damage analysis, the various time frames for the process under examination are separated and the information required for each time frame is obtained separately.
- The damage analysis is based on the normal case.

The first version, which is most commonly used in practice, leads to more time and expense for the preventive measures, but like Murphy's law states, "Anything that can go wrong will go wrong", and the most unfavourable situation will arise in an emergency. The second version leads to more time and expense to perform the BIA, set the priorities, develop business continuity plans, and perform the tests and exercises. The additional time and expense required for the second variant increases unproportionally as the number of different time frames increases and should only be considered when there are very few time frames. The third version means applying the normal risk to the entire time frame including the special time periods and events, but this version should only be used as an exception. Using this version can make sense, though, when the additional time and expense required to meet the higher requirements is uneconomically and unproportionally higher than the risk incurred by not taking the higher requirements into account within a very small time frame. If this version is selected, then the risk must be clearly and understandably documented and reasons provided for its selection in addition to the documentation of the selected strategy. The acceptance of the risk is to be confirmed in writing by the management.

D. Performing the damage analysis

Once all preparatory work is finished and the general conditions have been specified, the non-trivial task of performing the actual damage analysis begins. In this case, the effects in the organisation of the failure of each business process are estimated for each of the evaluation periods based on the damage scenarios, i.e. the damage resulting from the failure are determined.

The damage analysis should be performed in the corresponding organisational units since excellent knowledge of the business processes is required to perform the damage analysis. The business

continuity co-ordinators are responsible for performing the damage analyses and gather the corresponding information together with the person responsible for the process, and possibly together with the leader of the organisational unit.

The evaluations can be formulated as follows, for example: "The failure of a process results in direct economical damages that are categorised as low for up to 96 hours, normal for up to 168 hours, and high for 720 hours or more, while there are no effects due to legal violations". A format often used in practice is a table. The advantage of using a table is that it provides compact overview. Table 4 shows a simplified example of how a table for the damage analysis of a process could appear.

For the evaluation of the damage resulting from the failure of a business process, weighted sums based on the damage scenarios or the time (last line in Table 4) can be formed. The sums show the corresponding total damage from all weighted damage scenarios for each time period examined.

Process: Name of process									
Editor: Mr. Miller (Business continuity Co-ordinator)									
Contact person / Interview partner: Mrs. Maier (responsible for the process)									
Organisational Unit: Department 1									
Date of survey: Feb.11, 2008									
Time period:									
Recovery:	Restoration:				Maximum tolerable downtime:				
Recovery level:									
Evaluation periods / Damage scenarios	8 hrs.	24 hrs.	48 hrs.	96 hrs.	168 hrs.	720 hrs.	>720 hrs.	Weight	Com-ments
Financial consequences	1	1	1	2	2	3	3	5	
Impaired ability to perform tasks	1	1	2	2	3	3	4	3	
Violations of laws, contracts	*Not applicable to this process*							1	
Damage to image	1	1	1	1	1	2	3	1	
Weighted sum	9	9	12	17	20	26	30		

Table 4: Example of damage resulting "from the failure of a business process (1="low", 2="normal", 3=high", 4="very high")

If there are more precise specifications for the financial consequences of the amount of damage to be expected (e.g. from controlling), then this information can be added to the table. The specification of exact quantities suggests a precision that is not often actually achievable. For this reason, exact quantities should only be specified when the quantities are also consistent and reasonable. Exact quantities can also be useful additional information when performing the qualitative estimate.

One way to obtain a good overview of all business processes is to copy the results of individual processes into a general survey. Tables 5 and 6 show overviews of two different ways of presenting the damage resulting from the failure of several business processes in a survey. To improve the presentation, the number of damage scenarios and evaluation periods were kept to a minimum.

				Financial consequences				Impaired ability to perform tasks				Negative internal and external effects			
				Weight: 5				Weight: 3				Weight: 1			
Processes	**Recovery**	**Restoration**	**Max. tol. failure**	**24 hrs.**	**48 hrs.**	**96 hrs.**	**192 hrs.**	**24 hrs.**	**48 hrs.**	**96 hrs.**	**192 hrs.**	**24 hrs.**	**48 hrs.**	**96 hrs.**	**192 hrs.**
P1				1	1	3	4	1	1	2	3	1	1	1	2
P2				1	2	3	4	1	2	3	3	1	1	2	3
P3				1	1	1	2	1	2	3	3	1	2	3	4
…															
P12				1	1	2	4	1	2	3	3	1	1	1	1

Table 5: Example 1 of a survey of damage evaluations

For the specification of the recovery and restoration time objectives for individual processes, the resulting damage, the damage after a certain time frame (e.g. weighted damage after 192 hours in the example in Table 6), as well as the capacity available for recovery or restoration should also be taken into account. The times specified can be based on the increased damage from all damage scenarios, but also on the corresponding total damage for the process.

The results of the damage analysis from each organisational unit are collected centrally and consolidated by the business continuity officer.

Process	**Recovery**	**Restoration**	**Max. tol. failure**	**24 hours**	**48 hours**	**96 hours**	**192 hours**	**Weight**	**Damage Scenario**
P1				1	1	3	4	5	Financial consequences
				1	1	2	3		
				1	1	1	2	1	ge to image
				9	**9**	**22**	**31**		Weighted ∑
P2				1	2	3	4	5	Financial consequences

Weighted damage after 192 hours

				2	3	3	3	Impaired ability to perform tasks
				1	2	3	1	Damage to image
				9	**17**	**26**	**32**	Weighted ∑
P3				1	1	1	2	5	Financial consequences
				1	2	3	3	3	Impaired ability to perform tasks
				1	2	3	4	1	Damage to image
				9	**13**	**17**	**23**		Weighted ∑
…	…	…	…	…	…	…	…	…	…
P12				1	1	2	4	5	Financial consequences
				1	2	3	3	3	Impaired ability to perform tasks
				1	1	1	1	1	Damage to image
				9	**12**	**20**	**30**		Weighted ∑

Increased damage

Table 6: Example 1 of a survey of damage evaluations

Which method and which version of the damage analysis will be used must be decided individually by each organisation. A small or medium-sized organisation could reduce the number of evaluation periods and damage scenarios and apply the procedure described. The pragmatic approach for small organisations, which does not guarantee completeness or deliver objective, reconstructable results, would be to determine, classify, and prioritise the damage scenarios in a workshop in co-operation with the persons responsible for the relevant processes. The list of business processes must be created and the availability requirements must be specified for these processes at a minimum. If a security concept according to BSI Standard 100-2 was created, then this information is already available for most of the resources, and this information can then be used.

5.1.2.4 Specification of the recovery parameters

When performing the damage analysis or possibly shortly after its completion, the maximum tolerable period of disruption (MTPD), the recovery time objective (RTO) and the recovery level for each business process must be specified.

The maximum tolerable period of disruption (MTPD) of a process designates the time frame in which the process must be recovered so that the organisation does not enter a phase in which their ability to survive is threatened in the short-term or long-term.

The recovery time objective (RTO) specifies the time in which the process is intended to be recovered. The time frame specified for the RTO must be lower than the maximum tolerable period of disruption MTPD.

The recovery of a process, also referred to as business continuity, can be performed as follows:

- During emergency operations at any capacity and resource level in the original, normal operation environment

- Using alternate resources (e.g. at an alternate site)
- Using an alternative process with other types of resources and other procedures.

The recovery level and the process capacity required for stable emergency operation (e.g. 60% capacity) must also be specified in addition to the time of recovery.

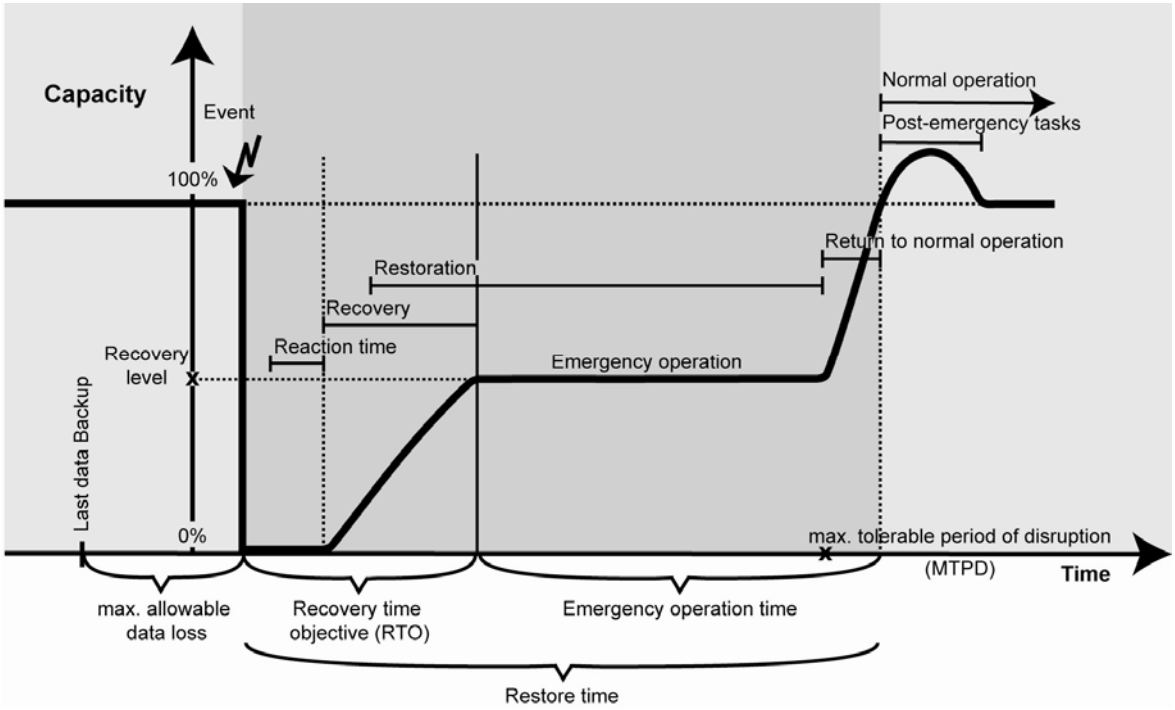


Figure 6: Recovery parameters

It makes sense when viewing the chronological order of the events in an emergency and the recovery procedure for a process to consider, specify, or take into account any additional activities and the times required to perform them (see Figure 6). For example, the recovery time consists of the time up to detection of the emergency, the reaction time (the time between when the emergency was reported and the initiation of the recovery measures, including escalation), and the actual time needed to recover the process. Since a process is seldom ready for normal operations immediately after recovery, it makes sense to specify the maximum tolerable period of emergency operation (MTPEO) or the maximum tolerable restoration time (MTRT). The latter is the sum of the recovery time and the maximum tolerable period of emergency operation.

The restoration time can also be longer than the maximum tolerable period of disruption MTPD since the occurrence of a problem threatening the existence of the organisation is delayed by the emergency operation. The time for returning to normal operation from emergency operation is part of the emergency operation time and must also be taken into account when planning. When normal operations are established again, it may be necessary to perform some post-emergency operation work, and the time required for this work is part of the normal operation time.

When specifying the maximum tolerable period of emergency operation MTPEO, the work required to be done after emergency operation must be considered as well. If the work required after a long period of emergency operation is so extensive that it cannot be performed within a reasonable time, then additional problems can arise.

5.1.2.5 Taking dependencies into account

The damage analysis and the specification of the maximum tolerable period of disruption, the recovery time objective, and possibly the restoration time objective, are based on the individual processes. The next step now is to take the dependencies between the business processes into account and correct the availability requirements, if necessary. As an option, it may make sense to give consideration to using an additional top-down approach to take the strategic goals of the government agency or company into account when assigning the recovery priorities to the processes.

Process dependencies

Dependencies between the business processes can lead to the necessity to adapt the recovery time objectives of individual processes. The size of the correction depends on the corresponding degree of dependency between the processes. If one business process requires the output or services from another process and this business process has a higher availability requirement than the processes supplying input, then a portion of this higher availability requirement may need to be inherited by the other business process. If the business process examined generates output, then the extent to which the output generated needs to be consumed within a specific time frame by subsequent processes must be examined. In this case, a higher availability requirement must also be assigned to the successor process to ensure that the process chain does not become "clogged" because the output cannot be taken on yet by the successor process. When examining the process dependencies, the outsourced processes must also be examined.

The degree of inheritance, and therefore the increase in the recovery time of the corresponding process, depends on the degree of dependency between the processes. This means that the higher the dependency, the greater the increase in or compensation for the recovery time. For this reason, it makes sense not only to differentiate between "independent" and "dependent" processes, but also to select a hierarchical dependency model. It is recommended to specify 3-6 levels for the degree of dependency. An example with 4 dependency levels could appear as follows: 1="very high", 2="high", 3="medium" and 4="low". A "low" degree of dependency means that no changes are necessary, while a "very high" degree of dependency means that the entire recovery time must be inherited. A definition of the degree of dependency must be specified for each of the intermediate levels. Figure 7 illustrates a highly simplified form of the procedure. For example, the recovery time objective of process GP5 is partially inherited by the preceding process GP4 since there is a "high" level of dependency between the two processes. The recovery time objective for process GP4 is therefore reduced from 168 hours to 48 hours. The recovery levels of the dependent processes should also be checked and corrected if necessary in addition to the recovery time objectives.

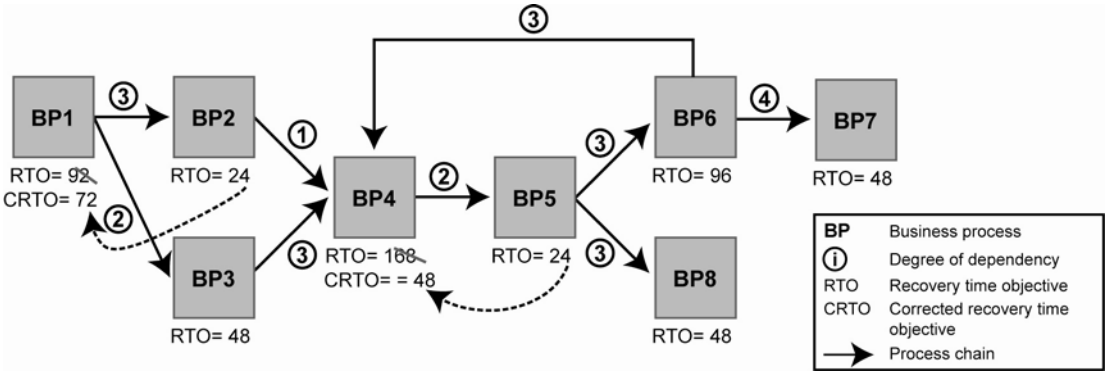


Figure 7: Inheritance of the recovery time objective by predecessor processes

This degree of dependency must be determined for both directions, meaning in the direction of the successor process as well as of the predecessor process. The specification of the particular degrees of dependency on the successor and predecessor processes should be made by the owner of the process when creating the process landscape before performing the BIA.

The degree of process dependency during normal operation may differ from the degree of dependency during emergency operation. If it is obvious in this phase of conception that there are differences and it is already known how emergency operations will be implemented, then the dependencies arising during emergency operation should also be examined. If the type of emergency operation is changed or only specified after finishing the emergency operation concept, then the corresponding dependencies should be re-examined and corrected, if necessary.

Process chains

In the damage analysis, individual business processes were examined as well as the effects of the damage caused by their failure. When examining the process dependencies, the availability requirements were inherited by the processes along the process chain depending on the degree of

dependency. In addition, it may make sense when there are high dependencies in individual process chains to examine the entire process chain and add the damage from each business process that would result from the failure of the entire process chain or parts of the process chain due to the failure of one or more essential processes. If the total damage caused by the failure of a process chain very quickly reaches a level that threatens the existence of the organisation, then it must also be checked if it makes sense to reduce the individual recovery time objectives in this chain.

Business goals

It makes sense for the organisation's management to introduce a top-down approach in which the business goals, the intentions of individual interest groups, and the core processes are also examined from a different perspective. The business goals of a government agency are usually derived from the tasks they are required to perform by law. The management level not only possesses knowledge of the current direction of the organisation, but also of the strategy for the future, and therefore of the corresponding development of the relevance and significance to the organisation of each of the business processes, lines of business, departments, or even corporate divisions.

For additional evaluation in a top-down approach, management can assign priorities to the interest groups and the business goals, and therefore to the process chains contributing to reaching these business goals. Processes needed to reach several business goals or business goals with a higher priority are assigned a higher priority than those processes only contributing to just one or more less important business goals. The additional evaluation performed by management flows into the overall evaluation of the individual processes and their recovery time objectives.

If this approach is used, then two more aspects should be taken into account:

- If a process is part of several process chains, then this fact will also have an indirect effect on the damage analysis.
- Only the process chains used directly to reach the business goals are examined, which means only the core processes are examined. The supporting business processes are not included in this examination.

Resource dependencies

When specifying the recovery time objectives for the business processes, the resources required for recovery and restoration should also be looked at. For example, it may be necessary but impossible to simultaneously recover a number of processes at a certain time since there is not enough personnel available at that time. Additional corrections to the recovery procedures and recovery time objectives may be necessary because of this.

Taking special time periods and events into account

If the strategy for handling special time periods (see section 5.1.2.3.C) in which different time frames were assigned to each of the processes examined was selected and the information required for each time frame in the damage analysis needs to be acquired separately, then these business processes must be given special consideration when assigning the priorities. The use of different time frames leads to more time and effort to determine the levels of inheritance of the process dependencies as well as to the need to create different priority lists for the various time frames.

5.1.2.6 Prioritisation and criticality of the business processes

If the recovery time objectives have already been specified and fine-tuned for the business processes, then the recovery time objectives are already in a certain order or have a certain priority. The recovery time objectives can generally be divided into individual recovery classes. A recovery order for the processes can also be specified in each of the recovery classes as well.

It is not necessary in the rest of the conception phase to specify the criticality, but this helps when talking about the criticality. The recovery time objectives or recovery classes can be used as the basis for specifying the criticality of the business processes since "critical" in business continuity management really means "time-critical". "Critical" therefore also indirectly means "damage-critical"

since the faster and higher the level of damage increases, the faster the processes need to be recovered. The specification of the criticality can be based on any useable criteria in addition to the recovery criterion (for example the maximum tolerable period of disruption or the total damage after x hours). Every organisation can decide for itself which criterion they will use to derive the criticalities and which (and how many) criticality categories they will use. Table 7 shows an example of a division into four criticality categories together with possible specifications. The numbers shown are fictitious and should not be used without further consideration.

Criticality Category	Recovery	Maximum tolerable downtime	Total damage after x hours	General information
"non-critical"	> 720 hours	> 504 hours	"low"	Failure has no effect or only minimal effects.
"less critical"	= 720 hours	= 504 hours	"normal"	Failure has effects.
"critical"	= 168 hours	= 240 hours	"high"	Failure has significant effects.
"highly critical"	= 4 hours	= 6 hours	"very high"	Failure or impairment leads to effects threatening the existence of the organisation.

Table 7: Example of criticality categories

It makes sense to specify the criticality categories so that the additional work required in business continuity management is concentrated on the business processes identified as being critical or higher to reduce the time and effort required for the subsequent worksteps to a reasonable level. When we mention "critical" business processes in the following text, we mean those business processes that will be examined further in the contingency concept and that have not been assigned secondary priority due to their low criticality in terms of time or damage. This selection of business processes therefore depends on the particular business continuity strategy of the organisation.

5.1.2.7 Determining the resources required for normal and emergency operation

A number of resources are needed to execute business processes. For the critical business processes, the resources needed for normal operation must be determined as well as thosewhich are used exclusively by one process, and those which are used by several processes. This information is needed to develop the recovery plans and should be determined carefully. If a security concept according to IT-Grundschutz is available, then a large portion of the information needed can be taken from the structure analysis. Some additional information on resources needs to be acquired since additional resource classes are of interest to business continuity management. The resources to be examined include:

- Personnel
  When executing business processes, employees to make decisions, operate machines, enter data, or perform other tasks are needed. If special qualifications or knowledge is needed for a business process, then this information should also be recorded in addition to the information on designated, possible, or missing substitutes. If special personnel is needed for recovery or restoration, then this information should also be acquired and recorded.
- Information
  Information includes the electronic data and paper documents needed to execute business

processes. A rough classification of the significance of the data to the business processes and identification of the essential data for the processes is useful when performing the rest of the examination.

When recording the resource "information", the maximum allowable loss of data (e.g. in the form of the number of transactions or age of the data) should be determined for the critical data. This value affects the data backup strategy in particular.

- Information technology
  IT is understood to be applications, hardware, software, communication connections (over the Intranet or Internet, but also over PBX systems), fax machines, and scanners, for example.
- Special equipment and systems
  Special equipment and systems includes, among others, production plants, security gates, medical devices, or control elements.
- Services
  If internal or external services are needed to supply an input to or provide resources for a process, then these services must also be noted. An example of a possible internal service is IT administration.
- Infrastructure
  Infrastructure includes, for example, the property, building, warehouse, production halls, car parks, file archives, server or office rooms, and workplaces, but also electrical, gas, water, or district heating networks, means of shipping and transportation (automobiles, lorries, trains, airplanes, etc.).
- Operating resources
  Operating resources are understood to be all resources not placed in any other category yet, for example raw materials or materials for production, office supplies, or office furnishings.

Resource			**Applications**								**Hardware**					**Infrastructure**					**...**
			email	**Database server(s)**	**Office application**	**SAP**	**EDI**	**AutoCAD**	**Calendar**	**...**	**Internet connection**	**LAN**	**File server 1**	**File server 2**	**...**	**Workplace**	**High rack**	**...**	**Telephone conn.**	**Fax**	**...**
Business process		**RTO**	4	92	24	…	…	…	…	…	48	…	…	…	…	…	…	…	…	…	…
	RTO	**kRTO**	4	18	24	…	…	…	…	…	48	…	…	…	…	…	…	…	…	…	…
Process GP1	92	72	1	1	4	1	3	-	4	…	3	1	1	-	…	1	-	…	1	-	…
Process GP4	168	48	3	-	1	-	-	-	3	…	-	1	-	1	…	-	1	…	-	2	…
Process GP5	24	24	-	1	1	-	-	1	-	…	-	1	1	-	…	-	-	…	-	-	…

Table 8: Example of resources recorded with specification of the degree of utilisation and the recovery time objectives

When determining the resources needed by a critical process, the corresponding degree of utilisation should also be evaluated and documented. The degree of utilisation indirectly specifies how the lack of

this resource will affect the continuity of the process. The higher the degree of utilisation of a resource, the greater the effect of the lack of this resource. A scale of three to five levels for the degree of utilisation has proven useful in practice. Possible degrees of utilisation based on the degrees of dependency between processes are, for example, 1="very high" (essential for the process), 2="high" (important for the process), 3="medium" (needed by the process), and 4="low" (see Table 8).

The single points of failure are also identified in this step or were identified earlier. The single points of failure are very critical resources whose failure would lead to the complete failure of the (sub)process. These single points of failure must be documented, and measures for securing them must be initiated as quickly as possible.

After determining the resources required for the normal operation, the resource requirements for emergency operation need to be determined. The following must be taken into account when determining these requirements:

- Not every business process allows emergency operation
- Emergency operation can consist of switching to alternative processes (for example switching from IT applications to paper or manual processing)
- Emergency operation can consist of operating the process at reduced capacity, with lower resource requirements, but therefore at lower input and output.

It must be documented for each critical process how emergency operation will be performed and which resources are required for this. If the recovery procedure is cascaded in several stages, then the resources necessary for each stage must be determined (see Table 9).

Process D		**Emergency operation**			
Resources	**Normal operation**	**= 2 hours**	**= 24 hours**	**= 48 hours**	**= 48 hours**
Workplace	8	2	2	4	8
Application H	8	2	2	4	8
Application B	4		1	2	4
Telephone connection	8	1	2	2	8
Experts	8	2	2	4	8
...					

Table 9: Example of resources documented for normal and emergency operation

It takes care and skill to determine which resources are needed because even though resources such as the workplace PCs or the Intranet are usually obvious choices, there are some operating resources that are only noticed once they become unavailable.

The resource determination can be performed together with the damage analysis or after prioritisation. The advantage of the first method is that nothing needs to be determined twice, and the contact persons responsible only need to be questioned once. The advantage of the second method is that the

resource determination is limited to the critical business processes and therefore takes less time and effort.

5.1.2.8 Criticality and recovery time objectives of the resources

The criticality and the recovery requirements for resources are generally derived from the criticality and the recovery requirements of the processes that utilise these resources. When passing the criticalities on to other processes via inheritance, it must be noted if the corresponding resource is used by more than one process and what degree of utilisation it has for each of the processes (see also Table 8). This means the same principles are in effect as for the inheritance of protection requirements according to BSI Standard 100-2, i.e. the maximum principle, cumulative effect, and distribution effect. The criticality of individual resources such as email, for example, can also be specified as "high" in a decision made by management regardless of the requirements derived from the business processes. Tight boundary conditions must be observed when specifying the resource recovery time objectives:

- If a resource is needed for emergency operation, then its recovery time objective depends on the recovery time objective for emergency operation. If it is not needed for emergency operation, then its recovery time objective depends on the latest restoration time objective for normal operation.
- Sometimes the resources needed by a process can be recovered in parallel, but some need to be recovered in a certain order. For example, data can only be restored after the corresponding applications (e.g. the database) have been installed. The applications can only be restored once the IT is available, which in turn requires the existing infrastructure to be restored (infrastructure RTO + IT RTO + application RTO including data restoration < process recovery time). For this reason, the recovery times of the resources are often lower than the recovery times of the processes. However, this depends on the type of emergency operation (which resources are needed for emergency operation) and the level of each stage when recovery is cascaded (when will what resources be needed and how much).

In addition, the extent to which additional equipping and startup times of the resources, which in turn leads to shorter maximum downtimes or dependencies between different resources, need to be taken into account must be clarified together with the people responsible for the resources.

The recovery requirements for the resources are often specified by the person responsible for the business process. In addition, a bottom-up approach can be used to evaluate the results. Practical experience has shown that it is advisable for the critical areas to also ask the people responsible for the resource or the users which resources they consider to be critical and how the failure of individual resources affects them. Since the person responsible for a process has an idealised perspective that is restricted to his business process, the perspectives from the other employees, which reflect their daily experience, can prove to be a valuable aid and control mechanism.

5.1.3 BIA report

The BIA report should contain all essential information recorded while performing the BIA, including the corresponding reasons. This means a BIA report should contain the following information at a minimum:

- Management overview
- Procedural model for the BIA (e.g. a reference to BSI Standard 100-4)
- Process landscape: processes, dependencies, process chains and their contribution to the business goals
- Organisational units examined and any business processes excluded from the examination
- General conditions, methods and approaches used when performing the criticality evaluation
- General conditions for the damage analysis
- Individual evaluations of processes

- List of the critical processes with a recovery priority
- Overview of resources for the critical business processes and their recovery requirements

The business continuity officer is responsible for creating the report. The report should be released in writing by the leaders of the individual organisational units and then submitted to top-level management for approval.

5.2 Risk analysis

The risk analysis performed in the context of business continuity management serves to identify threats that could lead to the disruption of business processes and to evaluate the associated risks. The goals of the risk analysis are the following:

- Make the risks present clear to the decision-makers
- If necessary, to develop suitable strategies and countermeasures for reducing these risks in advance and increase the robustness of the organisation
- Identify the scenarios for which individual business continuity plans need to be developed

Performing a risk analysis for business continuity management is optional since the goal of preventing risks has usually already been reached by the risk or information security management. If no other management discipline in the organisation has performed a risk analysis yet that completely encompasses the scope of business continuity management and all resources to be examined, then a risk analysis must be performed in the framework of business continuity management. The focus in this case is placed on the critical business processes and critical resources.

The classic approach to risk analysis is to identify the threats relevant to the organisation, to the process, or to the resource, and then perform a risk assessment. Risks are characterised in this case by the effects of the damage incurred when the threat actually arises, and the corresponding probability of occurrence of the threat. The following aspects should always be taken into account when performing a risk analysis:

- It is impossible to identify all risks. There is always at least one other risk that was not taken into account. For this reason, reasonable judgement should be used when performing the risk analysis, and an attempt to identify all risks that could ever be relevant should not be made.
- The probability of occurrence can only be estimated subjectively and roughly. Useful and well-founded numbers are only available for a few risks from the area of operational risks. Another problem is that it is often impossible to draw conclusions for the future based on events in the past since the general conditions can change very quickly.

5.2.1 Identifying risks

The first step in the risk analysis is the identification of possible threats and risks to the critical business processes. Threats are unders3ood to be dangers that can have a specific effect on the processes or resources due to existing vulnerabilities.

In contrast to the term “threat”, the term “risk” includes an assessment of the threat, and therefore expresses the damage that could be caused to the organisation by this threat.

While the BIA answers the question of what effects the failure of a process will have on the organisation, it is now necessary to answer the question of what the possible causes of the failure could be. In this case, risks at the process level as well as risks at the resource level need to be examined. A risk at the process level could be the failure of one or more (critical) resources, for example. A risk analysis at the resource level only looks for the possible causes of the failure of these critical resources.

Risks can be categorised based on different, independent characteristics:

- Internal / external risks
- Risks with a direct / indirect effect

- Risks that can /cannot be influenced by the organisation

A structured and systematic approach that also takes the various types of risk into account is also important for the identification of the risks. Known methods such as collection methods or search methods can be used for this purpose. The collection methods include, for example, checklists, SWOT analyses ("Strengths, Weaknesses, Opportunities, and Threats"), or interviews. Collection methods are especially well-suited for the identification of obvious risks. The search methods, though, are used especially to identify future or less obvious risks. These methods include the FMEA (Failure Mode and Effect Analysis), HAZOP (HAZard and OPerability study), fault tree analysis, morphological and statistical procedures, but also brainstorming, brainwriting, or the Delphi method. Since the individual methods have different strengths and weaknesses, several complementary methods should be used, if possible.

A good starting point for the identification of risks is the IT Grundschutz Threats Catalogues [BSIGK]. These catalogues contain a wide selection of threats for the following threat classes:

- Force majeure
- Organisational shortcomings
- Human error
- Technical failure
- Deliberate acts

To identify information risks at the resource level, the "Risk analysis based on IT-Grundschutz" procedure provided in BSI Standard 100-3 [BSI3] can be used. If a security concept was developed according to IT-Grundschutz, then much of the information from the analyses performed for this methodology can be used in this case as well. Additional risk analyses should be performed for those additional resources examined in business continuity management for which there are no results available from information security management.

5.2.2 Risk assessment

In an additional step, the risks identified are evaluated in terms of their relevance. To do this, the probabilities of occurrence as well as the damages to be expected can be estimated. This method has well-known problems, though. In particular, there are generally only useable numbers available for the probabilities of occurrence for certain areas, for example for natural disasters. For this reason, a qualitative approach should be used to estimate the probability of occurrence. Table 10 illustrates an example of a categorisation of the probabilities of occurrence for risks with four stages as well as the boundaries between each stage. Both the number of stages as well as the criteria must be specified by each organisation individually.

Improbable	Possible	Probable	Very Probable
Every 10 years or less often	About once per year	About once per month	Once per week or more often

Table 10: Example of probability levels

The estimate of the damages to be expected when business processes fail is available in qualitative or quantitative form in the BIA. If a quantitative approach was used to determine the damages, then it must be noted that the resulting numbers can only be considered rough estimates and can only be trusted to a certain point. It is also recommended to select a qualitative approach for the assessment of the potential damage.

To assess the risks, the probability of occurrence is put in relation to the possible damages, which are categorised as "low", "normal", "high", or "very high" as described earlier. One way to categorise the risks is shown as an example in the following table: "low", "medium", "high" and "very high". The categories must be specified by each organisation individually.

		Effect / Damage			
		Low	**Normal**	**High**	**Very High**
Probability	**Very Probable**	low	medium	high	very high
	Probable	low	medium	high	high
	Possible	low	low	medium	medium
	Improbable	low	low	low	low

Table 11: Example of a risk classification

The risks can be recorded and presented using different formats. The use of a software tool can be helpful. The following table shows one possible format:

Cause	**Risk**	**Scenario**	**Effect**	**Probability**	**Risk assessment**	**Weaknesses**	**Strategy**	**Measures**	**Responsible**
Cable fire Short-circuit Overheating	Fire	Failure of the Computer Centre	Very high	Possible	Medium	Split up room Install fire seals between ...	…	…	…
Failure of external power source Failure of internal electrical infrastructure …	Power failure	Failure of the Computer Centre	High	Possible	Medium	Only enough diesel available for 5 hours Only 50% of the servers are connected to emergency power supply …		Additional electrical generators	

Table 12: Example of a risk survey

A risk matrix is often used to provide an overview of the risks. A risk matrix can be especially helpful when selecting the particular risk strategy.

5.2.3 Forming groups and scenarios

To make the number of risks identified manageable for the subsequent steps, the risks should be

collected and grouped accordingly.

To identify specific preventive measures, the large number of risks must be made manageable. If the risks are examined at the process level, then it may make sense to place the risks associated with each business process examined in a group assigned to the corresponding process. At the resource level, the number of risks relevant to a resource are reduced by placing risks of similar type in the same group.

Since it is impossible to develop separate business continuity plans for each risk, scenarios should be developed. The risks can then be assigned to these scenarios. To keep the number of business continuity plans manageable, generalised and practical business continuity scenarios are worked out. The business continuity scenarios are developed based on the effects of the risks to the business processes. The use of the scenario technique is helpful during the development process. This technique examines the various chronological developments and escalation capabilities of the events (from the positive extreme to the negative extreme) and makes it possible to identify the risks associated with a particular business continuity scenario. When selecting scenarios to develop specific business continuity plans, it must be ensured that those business continuity scenarios that can cause high damages and whose probability of occurrence is high for the organisation are selected. A number of scenarios from 5 to a maximum of 15 scenarios has proven useful in practical applications. Examples of generic business continuity scenarios include:

- (Partial) failure of a site (e.g. due to flooding, large-scale fires, the area being cordoned off, failure of the access control system)
- Significant failure of information technology or the communication infrastructure
- Significant failure of systems or plants (e.g. in Production)
- A critical lack of employees (e.g. in cases of pandemics, food poisoning, strikes)
- Failure of service providers (e.g. suppliers, utility companies)

The business continuity scenarios can therefore be developed before or while performing the business impact analysis. Although the causes of a failure do not play a role when estimating the effects of the failure of a business process, it may be helpful to some of those responsible to imagine specific business continuity scenarios and then derive the effects.

5.2.4 Identifying risk strategy options

Risks can be accepted, transferred, avoided, or reduced. Strategy options are basic decisions regarding the handling of risks [BSI3]. For each critical business process and each risk, the suitable risk strategy options are determined and documented. The risk strategies then selected form the foundation for the selection of the continuity strategies later on. The residual risk remaining after implementing the particular risk strategy helps to decide for which business processes separate business continuity plans should be created.

When selecting the risk strategy, not only is the risk situation taken into account, but economical, operational, and technical aspects need to be taken into account as well, among other aspects. The possible risk strategies are described in more detail in the following:

Assuming risk

To assume an identified risk, the risk is simply accepted. This strategy option is often selected when a failure scenario with a low probability of occurrence and a low level of potential damage is identified.

Other reasons for accepting the risk could be that there are no effective countermeasures known for the corresponding threat or the total cost for effective countermeasures exceeds the value of the assets to be protected by the countermeasures, for example.

Risk transfer

A risk transfer is simply the transfer of the risk to another organisation. This can be done by signing an insurance policy or by outsourcing, for example. The direct financial damage can be lowered by signing an insurance policy since the resulting damages are completely, or at least partly, compensated

for (e.g. in case of a fire, flood, or theft). However, there is usually no compensation granted for the consequential damages resulting directly or indirectly from the failure of the affected business processes. This includes reputation damage, in particular. Before signing an insurance policy, any special terms and disclaimers should be taken into account. It must also be taken into account that there may be a long time to span financially before the insurance company pays compensation for the damage.

Another way of transferring risk is to outsource the affected business (sub)processes. This makes sense, for example, when the outsourcing partner is more able for economical or technical reasons to handle the risk. In this case, it must be considered that some risks, such as reputation damage or a limited ability to act due to dependent processes, are still assumed by the organisation. Furthermore, additional risks arise due to the new dependency on contracted service providers.

Risk avoidance

If a business process is assigned a high criticality due to having a special process flow, then a suitable strategy may be to change the process flows or the ambient conditions so that the corresponding threat becomes irrelevant. If a business process becomes unbearable for the organisation due to the risk identified, then it may even be necessary to stop this process and replace it with a completely new process. Risk avoidance always means that the probability of occurrence of the risk being examined or the damage resulting from its occurrence are reduced to zero.

Risk reduction

The most commonly selected strategy option is risk reduction, which means the probability of occurrence or the level of resulting damage is reduced. This can be achieved by implementing measures or by modifying the process flow.

For example, a very high concentration of risks is created when business processes are centralised in a computer centre, a practice used by many organisations today. The benefits gained due to the associated cost savings must be weighed against the higher level of risk incurred. Possible ways of reducing risk are therefore lowering the level of centralisation or distributing the risk among several computer centres.

5.2.5 Risk analysis-report

The risk analysis report should not only document the results, but also the method used to obtained them. This results in the following possible format:

- Management overview
- Method used for the risk analysis
- List of the risks with any groups already formed
- Results of the risk assessments
- Risk strategy options for the critical processes
- Selection of the risk strategies

The business continuity officer is responsible for the creation of the risk analysis report. The report is to be submitted to management and must be approved by management.

5.3 Determining the current state

The critical processes and their (critical) resources were identified in the business impact analysis. For the continuity strategy options and the strategy decisions developed in the following step, it is necessary to determine the current status of the contingency measures and the currently possible recovery time objectives so that it is possible to make a rough estimate of the action required for the various strategy options, and therefore of the associated investment costs. The current status also makes it possible to identify the measures that still need to be implemented after specifying the

strategies using a current state/target state analysis.

The determination of the current state can be restricted to the most important resources or areas (e.g. the critical business processes). A lot of this information can be obtained from the structure analysis performed when specifying the security concept according to BSI Standard 100-2. The resources not examined by the information security management should also be documented.

5.4 Continuity strategies

Business continuity and the recovery of the business processes can be realised in different ways. The alternative paths to a solution, i.e. the strategy options, differ in terms of their parameters such as the recovery time objective, the costs, and the reliability of the solution. The goal now is to identify the main alternatives and then selected the best approach for the organisation. To do this, the basic organisation-wide business continuity strategy, developed in the framework of initiating business continuity management and specified in the business continuity management policy, is applied to the process and resource levels in a top-down approach and then detailed.

5.4.1 Development of continuity strategies

The continuity strategy alternatives illustrate various ways of closing the gap between the target and current state of the contingency measures. The alternatives must meet the following basic conditions:

- Regulatory specifications
- The specified recovery time objectives for the processes and the resources must be met
- The costs of the alternative should be in an acceptable proportion to the damage expected from a failure per selected time period, which means they must be economically reasonable.

A general organisation-wide business continuity strategy is derived from the goals of the organisation and it's core business and is then specified in the business continuity management policy. The business continuity strategy forms the framework for additional considerations. The options for a continuity strategy are then specified at the institutional level together with general, basic principles. The following table shows an example of such a specification.

Strategy option	Description	Risk analysis
Minimum solution	Only the processes with maximum criticality are secured. The total cost of the measures are to be limited to ... . Security against the potential damage is obtained using insurance policies for the most part.	High residual risk
No solution	The processes with high priority are secured. The total cost of the measures is to be limited to	Medium to high residual risk
Medium solution	The most important core processes are secured. It must be ensured that internal capacities are used wherever possible to implement the measures.	Medium residual risk
Large solution	The critical business processes are comprehensively secures. High priority is assigned to abiding by legal restrictions and contracts as well as to preventing a loss of image.	Low residual risk

Table 13: Examples of organisation-wide strategy options

If an organisation-wide continuity strategy is specified, then it must be broken down to the process and resource level, and different courses of action must be specified in detail for the (critical) business processes and resources. The following table illustrates an (incomplete) example of strategy options at the process level. Detailed descriptions of possible alternative courses of action and additional examples of alternative measures can be found in Appendix A.

	“Computer Centre Operations” Process	**“Workplace Management” Process**
Minimal solution	Service contract for emergency operation	Internal solution: Release less critical workplaces for use as critical workplaces and home workplaces with the highest priority
Small solution	“Cold Standby” alternative (backup) computer centre	Solution with co-operational partnerships
Medium solution	“Warm Standby” alternative (backup) computer centre	Commercial “turn-key office building” service contract
Large solution	“Hot Standby” alternative (backup) computer centre	A second office building owned by the organisation

Table 14: Examples of strategy options for processes

5.4.2 Cost-benefit analysis

A basic goal of business continuity management is to secure business continuity sufficiently at an acceptable price. A cost-benefit analysis of the various strategy options can be used to select a good continuity strategy. To perform a cost-benefit analysis, the costs of the continuity measures must be analysed and compared to the benefits obtained. Numerous material and non-material factors (see also section 5.4.3) can increase or even decrease the benefits of a given strategy option. Since it is impossible to take all influencing factors into account, the cost-benefit analysis of the continuity strategies should be done using a pragmatic approach. The following explanations provide a general overview of such an approach:

Step 1: Determination of the damage to a process due to an emergency

The potential damage resulting from the failure of a process was already determined in the BIA. However, the BIA views damage not only in terms of financial damage, but also in terms of negative effects to the organisation, as is specified for a BIA. The benefits of a continuity strategy can be considered to be the ability of the organisation to keep damages low in an emergency by maintaining the process or recovering it as quickly as possible. The less damage resulting until the process is recovered or restored, the higher the benefits of a strategy option. Figure 8 shows an example of the possible resulting damage (dotted line), the generalised resulting damage for each evaluation period as determined in the BIA, as well as the recovery points RPSi for the various strategy options.

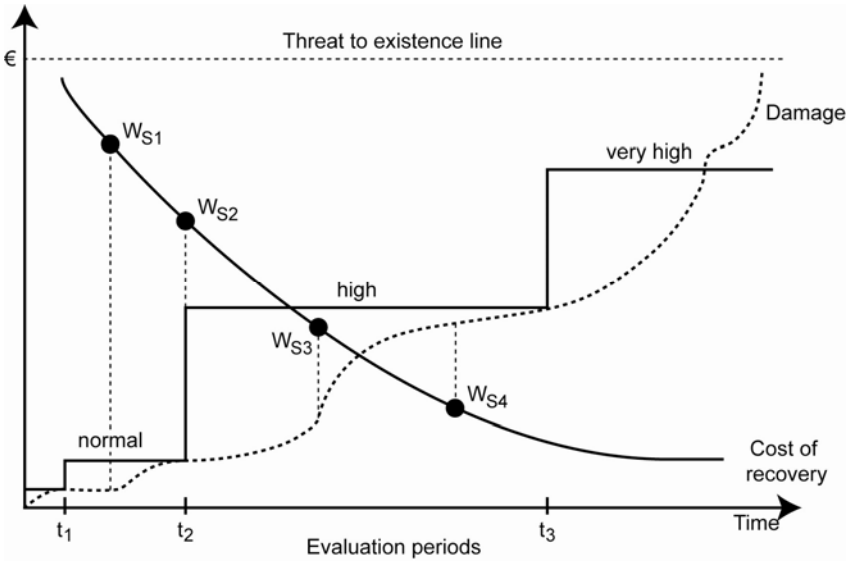


Figure 8: Resulting damage and recovery costs

Step 2: Determining the cost of the continuity strategy

In the second step, the cost of each strategy option is determined. The costs of the continuity strategies should be determined and estimated using the recognised financial planning procedures in the organisation. In addition to the purchasing costs, these costs include the recurrent costs for regular maintenance, training, leasing costs, or any contract costs (e.g. for reserving alternate workplaces from an external service provider). The current state of the business continuity measures and any gaps (which must be determined in a target/current state comparison for each strategy option) that need to be closed also play an important role when determining the costs.

Step 3: Preparing for the cost-benefit analysis

After determining the cost, the results of the previous two steps are summarised for use as an aid when making the decision. This summary should present the necessary costs to obtain a certain benefit. In general, shorter recovery time objectives lead to less damage, but also to higher investment costs, although strategy options with restrictive boundary conditions can break this rule. The following examples, which contain fictitious figures, sketch out several possible structures for a summary used to help make a decision. They do not cover all possible ways to secure a computer centre or the workplaces, and are not specified in full. A detailed description of alternative ways to secure a computer centre can be found in Appendix A.

"Computer Centre Operations" Process, MTPD = 10 days	**Recovery Time Objective**	**Costs**	**Damage until Recovery**	**Reliability / Boundary Conditions / Restrictions**
S1: Stand-by Computer Centre / "Hot"-solution: complete, redundant IT-infrastructure	< 6 hrs.	5 million €	low	very high
S2: "Warm" solution: own computer centre; all IT available; restoration from backups necessary in an emergency	6-24 hrs.	3 million €	low to medium	high

S3: “Cold” solution: some hardware needs to be purchased in an emergency; installation of the software and applications, and restoring data from backup copies	2-10 days	1 to 1.2 million €	medium-high	Residual risk: purchasing of hardware; max. RTO of 10 days corresponds to the MTPD and therefore no buffer remaining.
S4: “Emergency Computer Centre” service contract with service provider A	2 days	700,000 €	medium	Residual risk: capacity of the service provider available in an emergency
		1.3 million €	medium	Contract with preferential treatment
S5: Emergency Computer Centre” service contract with service provider B	2 days	500,000 €	medium	Residual risk: capacity of the service provider available in an emergency; Residual risk: reliability and image of the provider not adequate

Table 15: Example 1 – Cost-benefit analysis decision aid

“Computer Centre Operations” Process, MTPD = 14 days	**Recovery Time Objective**	**Costs**	**Damage until Recovery**	**Reliability / Boundary Conditions / Restrictions**
S1: Leased location	2 days	2000 € / workplace	medium	
S2: Purchasing of containers, if necessary	7-12 days	700 € / workplace	high	Residual risk: can only be set up on the company premises, and therefore not a solution when the company premises are unavailable.
S3: Home workplaces	12 hrs.	200 € / workplace	low	Currently only suitable for a maximum of 10% of the workplaces. Residual risk: availability of an Internet connection and of the dial-up node, computer and documents are located at the office workplace and not at the home workplace.

Table 16: Example 2 Cost-benefit analysis decision aid

Warning: The recovery time objectives and costs given in the examples are fictitious numbers and are only used to explain the procedure. Each organisation must determine or estimate suitable values for their specific applications and their requirements in terms of the workplace layout!

5.4.3 Consolidation and selection of the continuity strategies

The objective of the cost-benefit analysis is to provide a suitable list of possible continuity strategies to aid in the selection of the continuity strategy. However, the costs of the continuity strategies and the possible damages prevented by these strategies should be used as the sole criteria for the decision due to external factors and internal operational dependencies. Boundary conditions, restrictions, and availability estimates should always be included in the decision-making process.

The identification of internal dependencies can be co-ordinated internally. For example, the use of internal solutions as the continuity strategy requires a detailed examination. A detailed target/current state analysis should examine the following points at a minimum:

- Is it guaranteed that the recovery time objectives necessary in an emergency are fulfilled?
- Are there resource dependencies for resources needed by several processes at the same time?

External factors such as the sharing of rooms with neighbouring organisations or the significance of special time periods with higher recovery requirements for individual business processes may result in the need to reclassify the continuity strategy. External factors should be discussed and worked out together with the organisation’s management. For example, the bad reputation of a supposedly inexpensive service provider could result in an inadequate business continuity response in the organisation. The costs incurred as a consequence in this case would then justify the decision to select a more expensive solution. In addition, individual continuity strategies could provide additional benefits unrelated to business continuity management, for example by creating extra warehouse space.

As soon as the internal dependencies and outer factors are identified, a decision paper must be created and presented to the organisation’s management. The decision paper can also contain recommendations. It is management's job to specify the best strategies from their point of view. This decision is to be documented and confirmed in writing by the organisation’s management. All additional measures for business continuity management must be based on the selected strategies and specified in detail in the contingency planning concept.

The development and specification of the strategy are to be subjected to regular revision processes. If new strategy options or changes in external factors are identified, then a new cost-benefit analysis should be performed or a new consolidation meeting should take place.

5.5 Contingency planning concept

The contingency planning concept forms the foundation for the implementation of the continuity strategies. It describes the prevailing conditions and contains all information collected during the conception process. All organisational and conceptual aspects as well as all business continuity management measures and tasks that do not contribute directly to the response to an emergency should be described in the contingency planning concept. These aspects include:

- Preventive measures that reduce the damage from or probability of occurrence of risks and increase the resistance of the organisation by raising the crisis threshold
- The measures implemented to enable quick and sensible response to an incident

For this reason, a contingency planning concept must be planned carefully, implemented carefully, and revised regularly. The information needed immediately to respond to an emergency, for example contact information or instructions, is described in the business continuity handbook (see section 7.4). Together, they form the contingency concept.

5.5.1 Detailed concept, security, and controls

The individual preventive measures for prevention and the implementation of the continuity strategies must be specified. In addition to the solutions for emergency operation, solutions for a return to normal operation and for the post-emergency phase after resuming normal operations must also be worked out.

Both aspects, i.e. security and data protection, should play an important role when creating the detailed concept and the business continuity handbook. Security is understood to be information security and personnel security as well as operational reliability. If classified materials are processed in the affected business processes, then the Industrial Security Officer must be involved. It must be ensured that security is guaranteed during emergency operations as well as when returning to normal operations. For example, it must be ensured that legal requirements for the protection of the employees are fulfilled and that the confidentiality, integrity, and availability of information is guaranteed. For this reason, it makes sense to work closely with the responsible security personnel (e.g. the IT Security Officer, person responsible for operational reliability, etc.). The task of creating a security concept for emergency operation is not an original task of business continuity management or of the business continuity officer.

The IT Security Officer is in charge of creating and implementing a corresponding information security concept for the processes, systems, and business continuity management measures for the IT area, provided that the information security concept is not already part of the current security concept. In the information security concept, the business continuity processes required for emergency operation, but also the processes in the recovery phase, the processes for returning to normal operations, and the post-emergency tasks are examined, and the confidentiality and integrity of the processes and the information processed are ensured in each intermediate step. For recovery or restoration plans, this can mean, for example, that the steps must be performed in a certain order. For example, the confidential data in an application can only be restored after the security of the network is guaranteed by a completely recovered security gateway and additional security safeguards. If compromises or trade-offs in terms of information security or data protection in the recovery phase, during emergency operation, or when returning to normal operations need to be made, then these compromises or trade-offs must be documented, the risks incurred because of taking these compromises or trade-offs must be pointed out, and the organisation’s management must approve these compromises and trade-offs by signature.

The specifications of the internal auditing department of the organisation should also be followed as well when creating the detailed concept. It must be examined to what extent the controls established to maintain proper operation during normal operations, to defend against industrial espionage, or to detect cases of misuse are essential or non-essential to emergency operation. It is therefore recommended to work in co-operation with the internal auditing department so that it can check the emergency operation processes in these terms and release them when approved.

5.5.2 Content

The contingency planning concept is created by the business continuity officer in co-operation with the business continuity co-ordinators and the contingency team. The organisation’s management is responsible for the strategies specified in this concept and must therefore approve and release the concept as well.

The contingency planning concept should contain the following points at a minimum:

Procedural model and implementation

The contingency planning concept specifies a clearly defined framework for determining how to establish, set up, and monitor the ability to continue business in an emergency. It must precisely describe how to integrate each phase of business continuity management into the existing structures of the organisation and how to control and monitor the activities of business continuity management. The effectiveness and efficiency of the business continuity management system must be checked regularly. An independent testing procedure must be set up for this purpose.

Definition of a malfunction - emergency - crisis

As soon as an emergency is declared, the normal business processes are replaced by the processes for business continuity response in the affected area. However, not every incident initially declared an emergency is actually a real emergency, but it is important for every organisation to define for itself when a malfunction, emergency, or crisis is present and who is authorised in the organisation to decide this.

Preventive measures

The preventive measures specified, for example the alarm technology, alternate sites, or the relevant agreements with external service providers in case of an emergency (see also Appendix B), must be documented. Preventive measures relevant to business continuity management but which have already been covered by the information security concept should be listed with references to the corresponding information security or risk management documents.

Glossary

It is essential to establish a common ground of understanding of the goals and business continuity management measures in an organisation. To do this, all terms need to be clearly and uniformly defined and documented in an understandable manner. A glossary containing the most important terms relating to business continuity management should be created to reach this goal.

Contents of the contingency planning concept

The contingency planning concept should contain the following points at a minimum:

General information

- Specification of the person responsible for the documents
- Classification of the document and of the approval procedure
- Specification of the scope, version
- Document recipients and distribution paths
- Document structure and relationship to other relevant documents
- Index of abbreviations, glossary

Organisation and procedural model

- Definition of the terms “malfunction”, “emergency”, “crisis”
- Acceptance of responsibility by the management
- Goals, responsibilities, authorities, and integration into other management systems of the organisation
- Integration of business continuity management into all relevant business processes and all specialised procedures and projects
- Description of the contingency planning and business continuity response organisation
- Description of the operational structure and the implementation

Business process and damage analysis

- Business continuity scenarios and their effects
- Critical business processes and their recovery requirements
- Priority list
- Continuity strategies

- Cost of contingency planning
- Residual risks remaining

Organisational and technical preventive measures

- Specification of general alternate sites and their requirements
- Alarm procedures
- Description of risk-reducing measures
- Data backup
- Alarm technology
- Agreements with external service providers
- …

Permanent integration of business continuity management into the government agency or company culture

- Awareness-raising and training of the employees
- Integration of maintenance, testing, and monitoring processes in the existing internal processes

Maintenance and monitoring

- Continuous improvement of business continuity management through exercises and test runs
- Maintenance and revision of the contingency planning and business continuity response measures
- Description of control and monitoring of the business continuity management system

Before creating the contingency planning concept, itshould be considered organising and dividing the contingency planning concept into individual modules. The division can be based on the corresponding target group requiring individual sections for implementation. It should also be considered if division into a general section and main section makes sense in your organisation. The general part only contains general, basic business continuity management principles and is therefore also suitable for use in acquiring customers or co-operation partners. The main part contains the internal, confidential, detailed information required for implementation.

5.5.3 Publication and distribution of the contingency planning concept

The contingency planning concept is release by the management, published by the business continuity officer, and distributed to the group of authorised recipients. It is important that all persons participating in contingency planning are familiar with the contents of the contingency planning concept and can understand the contents at all times. It must be examined if any other people, for example from the business continuity response teams or co-operation partners, need the entire contingency planning concept or just excerpts from it to do their work.

Since a contingency planning concept can contain confidential information but is also needed to secure many business processes, it must be specified who will receive the contingency planning concept and how it should be classified. The answers to these two questions can differ greatly depending on the organisation.

5.5.4 Updating the contingency planning concept

The business continuity officer is responsible for continuously updating the contingency planning concept and ensuring it is complete. The contingency planning concept should be checked to see if it is up-to-date at regular intervals and modified, if necessary. When checking, it should also be examined if any business goals or tasks, and therefore business processes or production procedures, have been changed or if the organisational structure has been revised.

6 Implementation of the contingency planning concept

This chapter describes how to plan, execute, supervise, and monitor the implementation of the contingency measures. Since some areas of the contingency measures and the security safeguards overlap, the implementation should be co-ordinated with the information security management just like when developing the concept.

There are usually only limited resources in terms of money and personnel available to implement the measures. The goal of the steps described in the following is therefore to achieve the most efficient implementation of the intended measures possible.

6.1 Estimating the time and expense

An initial, rough estimate of the cost of the preventive measures was already made when developing the continuity strategy options. After deciding to use a certain strategy and detailing this strategy in the contingency planning concept, a detailed list of the expected costs can now be made.

Since the budget for implementing preventive measures is almost always limited, the cost of investment needed to implement each measure should be recorded together with the associated time and expense for the required personnel. When recording theses costs, a differentiation between one-time and recurrent investment costs and personnel expenses must be made.

If it becomes clear during this phase that the selected measures are not economically feasible, then it should be considered if there are more economical measures that can be used as replacements or if the residual risk incurred by not implementing the measures is acceptable.

If there are not enough resources available to implement the contingency planning concept, it makes sense to prepare a presentation for the decision-makers illustrating the results of the BIA and risk analysis. The effects resulting from unimplemented preventive measures should also be presented in order according to the priorities of the business processes. In this case, both the current state of security of the particular business process as well as the residual risk resulting from not securing the business process play an important role. Furthermore, it makes sense to prepare a list of the expected time and expense to implement the missing measures. The resulting residual risks should be described and submitted to management for a decision. In connection with this presentation, a decision on the budget and on the implementation priorities for the business processes should be made. Since management bears the responsibility for the consequences, additional steps can only be taken after management has decided if the residual risks are acceptable to the organisation.

6.2 Specification of the order of implementation of the measures

If the existing budget or personnel resources are insufficient to immediately implement all measures, then an order of implementation must be specified. When specifying the order of implementation of the measures, the priorities specified when securing the business processes must be taken into account. In addition, the following aspects should also be taken into account:

- If a business process contains a single point of failure, i.e. a point whose failure leads to the failure of the entire business process, then the elimination or securing of this single point of failure must be given the highest priority.
- If a business process contains individual subprocesses which are secured with a lower level of security than the rest of the subprocesses, then these subprocesses should be given preferential treatment to obtain a uniform level of security in a process.
- For some measures, there are logical relationships that require a specific chronological order.
- Some measures affect a large area, while the effects of others are limited to local effects. It often makes sense to handle those measures affecting a large area first.

The decision regarding which preventive measures will be taken immediately and which will be delayed as well as where residual risks will be accepted should be documented carefully for legal

reasons. In case of doubt, additional opinions should be surveyed and these opinions documented as well to prove the duty to take good care was fulfilled in case of a legal battle later on. The selection and order of the measures suggested from a technical point of view must be examined by the decision-makers and confirmed in writing.

6.3 Specification of the tasks and responsibilities

It must specified who is required to implement which preventive measures and by when. Experience has shown that the implementation will be delayed significantly or skipped completely without such specifications. In this case, it must be ensured that the person named responsible has the skill and authority necessary to implement the measures and that he is provided with the necessary resources.

Likewise, it must also be specified who is responsible for monitoring the implementation and who is to be reported of the completion of the implementation of each measure. The business continuity officer is usually informed of the completion. The progress of the implementation of the measures should be checked regularly so that the implementation tasks are not delayed.

The implementation plan now finished should contain the following information at a minimum:

- Description of the measures
- Implementation schedules
- Budget framework
- Person responsible for implementation
- Person responsible for the monitoring the realisation

6.4 Measures accompanying the implementation

It is particularly important to design the measures accompanying the implementation in advance and to include them when planning the implementation of the measures. These measures include measures such as awareness-raising and training programs in particular. These programs should illustrate the role of the employees in business continuity management as well as the necessity for business continuity management.

If the employees do not receive adequate training, then they could delay the reaction to an emergency. Inadequately informing the employees often leads to employees taking a hostile attitude.

7 Business Continuity response and crisis management

Since it is impossible to completely eliminate all risks through risk-reducing measures, contingencies must be implemented for the residual risk remaining. This is done by establishing a business continuity and crisis response (also referred to as crisis management) that is activated in case of an emergency or a crisis. This includes the identification and analysis of possible emergency and crisis situations, the development of response strategies, and the introduction and monitoring of countermeasures. When a damaging event that impairs business continuity occurs, the local business continuity response or the crisis management is activated depending on the scale of the event. Crisis management in the framework of business continuity management is part of the organisation-wide general crisis management and represents a higher escalation level of business continuity response.

A functioning business continuity response and crisis management system requires an organisational structure and an operational structure. The organisational structure was presented in section 4.3.2. A crisis team is required for the business continuity response as well as for crisis management. The difference between an emergency and a crisis lies in the resulting responsibilities and work methods. While an emergency can be handled using business continuity plans for the most part, a crisis requires a different approach. Due to the uniqueness of each crisis, the requirements placed on the work performed by the crisis team are higher for a crisis than for an emergency. Large organisations sometimes make a distinction between the business continuity team and the crisis team. For reasons of simplification, we do not make this distinction and consider the business continuity team to be a local crisis team.

The description of the operational structure contains the procedures to follow after a damaging event occurs, starting with the reporting of an emergency, continuing through escalation and restoration, and up to de-escalation. In the following, the most important structures and steps for business continuity response and crisis management are described. In this case, it must be noted that there is no fixed procedure to follow when a damaging event occurs, and the response must be adapted to the particular situation. This is reflected in the organisational structure activated as well as in the operational structure.

7.1 Operational structure

The basic steps and tasks to perform when an emergency or a crisis occurs can be illustrated as follows:

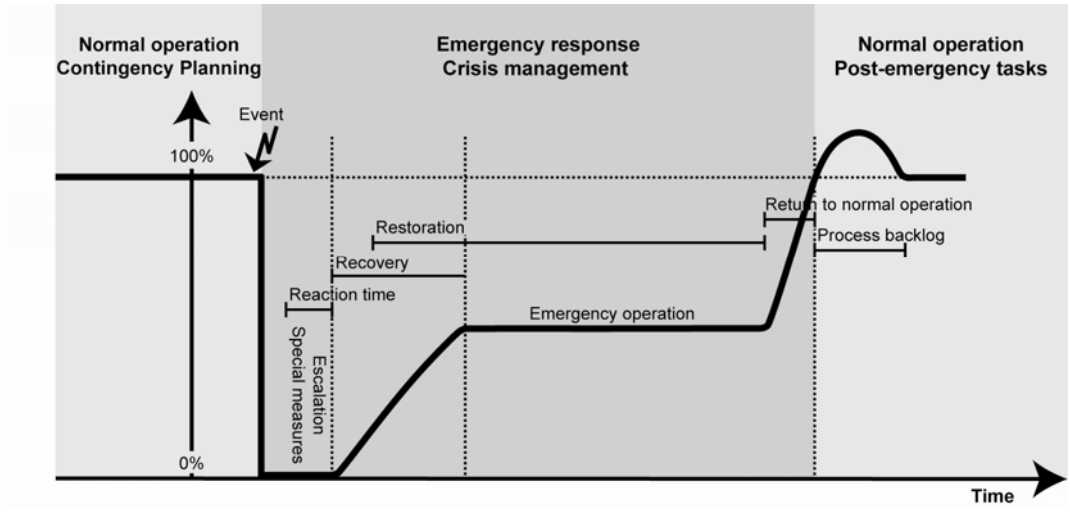


Figure 9: Phases of the response to an emergency or a crisis

When a damaging event occurs, the reporting of the event triggers the business continuity or crisis response process. If necessary, immediate measures are initiated and escalated to the crisis team leader when an emergency or crisis threshold is exceeded. The crisis team leader assesses the situation, determines what has happened, and what possible effects can be expected. Depending on the seriousness of the event, the specialised department is informed of the malfunction, the local business

continuity team is activated to respond to the emergency, or the crisis team is called up to manage the crisis (see Figure 10).

When the crisis team meets, it makes decisions with the goal of minimising the damage and enabling the fast resumption of operations. It issues corresponding instructions to the business continuity team and monitors the situation. It also ensures internal and external crisis communication is possible. After resuming operations or recovering to the normal situation, it de-escalates the business continuity response, and normal operations are restored using the corresponding organisational structure.

7.1.1 Reporting, alarming, and escalation

The quick and suitable flow of information is also decisive to the ability to successfully respond to an emergency or a crisis. For this reason, it is particularly important to specify paths and procedures for reporting, escalating, and triggering alarms in case of an event.

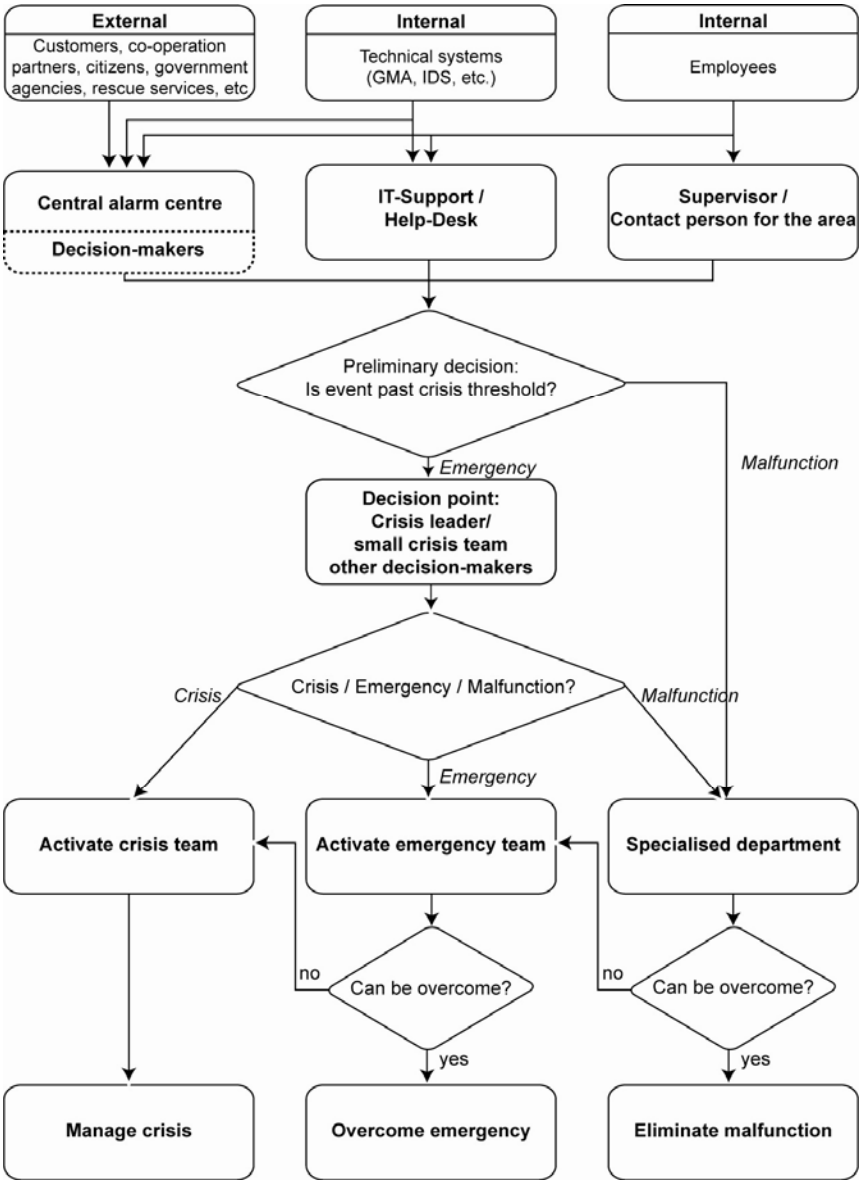


Figure 10: Alarming and escalation

Central alarm centre

Unusual or critical events can be reported by external or internal personnel. The reporting paths must be clearly specified to ensure that all alarms are sent to the central alarm location responsible. The central alarms one at one location or a group of different locations (CERT, IT Support, reception desk, department head, control centre, emergency centre, etc.) for different types of events (e.g. fire alarm,

failure of a service provider, financial crisis, IT crisis). In any case, these locations must be clearly specified, and all employees (and external personnel, if necessary) must be informed of these locations.

The central alarm centre should be accessible around the clock. Outside of normal business hours, access can be provided using various measures such as working in shifts, outsourcing, or automatic forwarding of alarms to an on-call emergency service.

There are two types of internal alarms; alarms generated by employees and alarms generated by technical systems (e.g. alarm systems). External fault alarms are typically generated by customers, business partners, citizens, government agencies, or even support services.

The alarm messages sent by people to the central alarm centres should use a predefined format to ensure that they contain the information necessary for an initial evaluation. The alarm messages should be brief, clearly separate the facts from any speculations, and contain the following specifications at a minimum:

- Time and location of the event
- Person or location reporting the alarm
- Any affected persons, areas, or processes
- Possible causes or triggers of the alarm
- The effects currently felt

If necessary, the central alarm centre initiates immediate measures such as alarming fire and rescue services or alarming the employees of the emergency using an acoustic and/or visual signal.

Alarm or escalation levels

As soon as a damaging event passes a certain threshold, management of the event is escalated to those responsible for managing such events. Alarm or escalation levels form the basis for the decision to escalate the alarm. These levels must be defined, the criteria and threshold values must be specified, and decision-making aids must be developed in advance. In extreme cases, an organisation can decide to work with just one escalation level, which means escalation directly from normal operations (including fault management) to a crisis. Usually, though, an escalation model is used in which several stages are defined. This permits more specific reactions to incidents.

Escalation levels can be defined as follows, for example:

Escalation level			Examples
1	Green	Normal operation	--
2	Yellow	Fault alarms	Events that need to be reported, checked, documented, and eliminated, if necessary.
3	Orange	Early warning	Events initially requiring defensive or risk-reducing measures such as extinguishing a lone fire.
4	Red	Emergency	Events that seriously impair business operations and cannot be eliminated in the required time any more.
5	Red	Crisis	Events with the potential to become a crisis that requires a higher level of co-ordination and that endanger lives or the existence of the organisation.
6	Red	Disaster	Large-scale damaging events not restricted to the organisation alone.

Table 17: Possible escalation levels

Alarming and escalation procedure

When specifying the escalation and alarming procedure, itmust be defined who is allowed to escalate, to whom the alarm will be escalated, and who needs to alarm whom. Depending on the qualifications of the central alarm centre, the alarm centre decides which escalation level is currently necessary based on the decision-making aids, or it informs a decision-maker who then makes this decision. If the alarm is due to a malfunction, then the alarm is escalated to the corresponding specialised department. If an emergency threshold is exceeded, then the alarm is escalated to a decision-making body that decides how to respond to the emergency. Alarms can also be escalated to the business continuity response team by the specialised departments, for example the IT fault management, or by the person responsible for the business process. In these cases, the alarm is usually due to slowly developing malfunctions that eventually exceed a threshold and turn into an emergency.

If the alarm was escalated to the decision-making body, then this body must decide if the alarm is just a malfunction, or if it is due to an emergency or a crisis. The decision-making body can consist of just the crisis team leader, any other person assigned to this task (e.g. from management or the board of directors), or a small group of people, for example from the crisis team. An advantage of allowing the crisis team leader to make this decision is that an additional escalation level is unnecessary and he has the knowledge and authority necessary to assess such situations. One disadvantage of this solution is that the crisis team leader could declare a crisis and therefore take command of the organisation. This hypothetical problem can be eliminated by introducing one or more monitoring bodies as a safeguard. These bodies are able to examine and revoke the crisis declaration and then de-escalate, if necessary. The examination can be triggered by anyone.

If the decision-making body decides that the alarm was due to a malfunction, then the alarm is de-escalated to the corresponding specialised department for elimination of the malfunction. If it decides there is an emergency, which means a local damaging event, then the necessary business continuity teams and the local business continuity response are alarmed to respond to the emergency. If the damaging event is a large-scale event requiring a higher level of co-ordination and cannot be eliminated using the business continuity plans alone, then a crisis team is assembled whose composition depends on the situation. It may be necessary to inform other locations, for example other branch offices, agency partners, or health services. The leader of the crisis team also decides if the alarm needs to be escalated to a higher level in the management hierarchy.

To trigger and escalate alarms, escalation path plans must be available, and it must be possible to reach the crisis team members as well as the external locations that need to be informed. This also includes descriptions on how to proceed if individual members of the crisis team or the business continuity team cannot be reached. A graphic containing the relevant information (for example in the form of a data flow chart) makes it easier to intuitively understand the information and provides a clear overview. This can be beneficial, especially in stressful situations. The internal areas and external locations who need to be alarmed should be alarmed as quickly as possible. For this reason, consideration should be given to the use of a software support tool, especially in large companies or when a large number of locations need to be informed.

Type and manner of alarming

It must be specified how to trigger and escalate alarms. This can be done in the form of a chain in which one person alarms one or more other people, or in the form of a star topology in which one central location alarms everyone at the same time.

Likewise, it must also be specified when to forward an alarm as well as when the crisis team just needs to be informed and when it should be alarmed.

Some basic principles should be observed and followed when issuing alarms. The message sent to the people responsible for the business continuity response should be short and concise. Discussions and long explanations of the situation are to be avoided when issuing alarms. It should be easy to discern from the message what steps the person alarmed needs to take, e.g. to go immediately to the crisis team meeting room. The person alarmed absolutely must respond promptly to the call. If the person to

be alarmed lives together with other people in the household who could answer the telephone, then these people must also be instructed in advance by the contingency organisation of what to do if they answer the telephone during an alarm. The person alarmed must completely document the alarm. This includes the following specifications:

- Who has been alarmed
- Who issued the alarm
- When the alarm was triggered
- Who was reached
- What was the result

Technical support is needed to issue an alarm. This support must be guaranteed, especially in case of an emergency or a crisis. Technical support generally comes in the form of land linesl, cellular phones, Internet telephony (VoIP), radio receivers (also referred to as pagers), and radio or satellite communication devices. In this case, the use of systems that are able to detect if the target person was reached and if the message was received should be preferred to issue the initial alarm. The use of SMS (Short Message Service) is only partially suitable for alarming because it is usually impossible to receive a reply immediately and guarantee a certain transmission time.

In case of a disaster in which the telecommunication and/or Internet infrastructures are disrupted, alternative communication and alarm paths should be considered and planned since common alarm systems require either the Internet or the telephone network (and possibly both), depending on if the system was implemented as a separate internal system or a third-party service provider was contracted for this purpose.

7.1.2 Immediate measures

After an event is reported, the first step in the business continuity response is to introduce immediate measures, provided that such measures are necessary. Examples of immediate measures include extinguishing fires, evacuating buildings, or rescuing people. These measures are initiated even before escalating the emergency. The idea is to prevent large amounts of damage and, in particular, to prevent injuries to people that would occur if time was wasted.

The corresponding instructions and specific tasks must be specified and documented in advance. They must clearly state who is allowed to initiate and carry out which immediate measures. The roles to fill in case of an emergency such as first-aid providers, company rescue team members, fire-fighting assistants, evacuation helpers, or business continuity response team members must be specified, and someone must be assigned to each role. These people are alarmed immediately and take action independently at the site of the emergency.

Since the trade unions have already enacted the corresponding legal requirements, which need to be fulfilled in every organisation, corresponding instructions for immediate measures should already be available in every organisation. The corresponding organisational safeguards are to be integrated into the operational structure of the business continuity response in a suitable form. The information and instructions required are to be provided in the business continuity handbook.

7.1.3 Crisis team meeting room

When an emergency is escalated to a crisis, the members of the crisis team must be informed immediately and must convene at a location specified in advance, which is referred to as the crisis team meeting room. This space, which is also referred to as the situation centre, serves as the working environment for the crisis team. This means there are special requirements to be fulfilled in terms of its location and the equipment provided there.

The location of the crisis team meeting room must be selected so that it is easy to reach by the members of the crisis team in an emergency or a crisis. It should be located centrally at the main site of the organisation. An alternative location should also be available in case the crisis team meeting room at the main site cannot be used. The alternative location should be located far enough away from

the main site considering the possible emergency scenarios. Locations such as branch offices, if any exist, but also rented space, office containers, or mobile alternatives can be used as the alternative location. The following points should be considered, among others, when selecting the crisis team meeting room and its equipment:

- Sufficient space: The rooms should provide enough workplaces as well as separated meeting areas that can be darkened for presentations. For longer crises, social areas such as eating and resting areas, toilettes, washrooms, and smoking areas should be provided, if necessary. The sizes of the rooms selected should not just be able to hold the estimated number of personnel needed because the number of personnel actually needed depends on the type of event.
- Access: Access to the rooms must also be available after regular office hours.
- Security: Access to the rooms is to be protected using a suitable access protection system. Depending on type of crisis, the confidentiality of the information received and of the meetings plays a more or less important role. For this reason, the crisis team meeting room should be equipped with privacy protection and must be secured against eavesdropping, if necessary.
- Technical equipment: The corresponding technical equipment is necessary to acquire, process, and present information. Such technical equipment includes, among other equipment, networked computers, beamers, scanners, copiers, printers as well as mobile storage media for transporting and exchanging information. The IT infrastructure of the crisis team meeting room should not be dependent on the Intranet since it may not be available any more during a crisis. This infrastructure includes, for example, an email server, a public key infrastructure, or even databases containing the necessary information. Note, though, that fax machines, radios, televisions, or video recorders are also useful devices. Mobile telephones, possibly battery-operated analogue telephones or, when the mobile phone and land lines networks fail because of the disaster, satellite telephones should also be available in addition to normal telephones.
- Climate control: An air conditioning and climate control system improves working conditions and reduces stress. It should be possible at all times to regulate the climate.
- Redundant power supply: A redundant power supply should be reserved for the technical devices, including the telephones.
- Redundant telecommunication and Internet connections: To be able to call up information from the Intranet or even the Internet, it is recommended to have a redundant connection to the Internet and to use several different lines of communication.
- Other equipment: In addition to the technical equipment, office materials, consumables (e.g. printer cartridges, batteries), tools for presenting information (e.g. flipcharts, chalkboards), and tools for acquiring and processing information (e.g. maps, reference books, and telephone books) will also be needed. A shredder should also be available to destroy confidential documents. Depending on what types of damaging events were identified as being possible (e.g. the release of chemicals into the environment), it may be necessary to provide a sufficient number of protective suits, for example.
- Food and waste disposal: The provision of food for the crisis team as well as waste disposal should be taken care of.

The operability of the room and its equipment is to checked regularly.

Special challenges are presented by crises in which the ability of the crisis team members to meet in the crisis team meeting room is limited, unnecessary, or even undesired, for example in the case of a pandemic. For this case, an alternative which permits the team members to work together while at separate locations should be developed.

7.1.4 Tasks and authorities of the crisis team

If an event is escalated and the crisis team is activated, then the actual response to the emergency or crisis begins when the members meet together in the crisis team meeting room. The crisis team specifies which areas are affected by the crisis (e.g. buildings, branch offices, several sites). It only has

authority over these areas.

One of the core tasks of the crisis team is to make decisions and co-ordinate the business continuity teams to respond to the emergency or the crisis. The main difference between an emergency and a crisis is that an emergency can be managed for the most part with the help of business continuity plans. A crisis requires more extensive authorities. A crisis is a unique event that cannot be handled based on examples and which requires quick and qualified decisions.

The main tasks of the crisis team include:

- Acquiring, evaluating, and preparing information
- Surveying and evaluating the current situation
- Developing handling options and evaluating them in terms of their likelihood for success, consequential risks, and general conditions
- Specifying measures
- Assigning the task of performing and monitoring the individual business continuity measures to the business continuity team
- Examining the effectiveness of these measures and implementing corrections if the measures did not lead to the desired result
- Communicating with partners, employees, government agencies, and the media

If the emergency will take a long time to manage, then the crisis team must organise its procedures and structures, but also the necessary infrastructure by itself. This includes, among other items, organising shift changes and supplying the employees with food and resources.

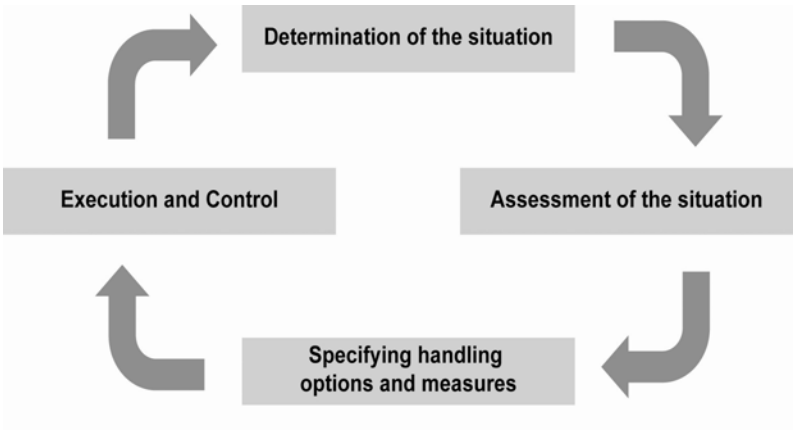


Figure 11: Response process

Assessing the situation and obtaining information

Comprehensive information is needed to assess a situation. A situation refers to the factors and conditions describing the damage event and the damage prevention measures, for example the type and scope of impairment, any damage already created as well as how the damage will develop, the number of persons affected, any acute dangers, the time of the event, and the state of the supply and traffic network.

To assess the situation, the crisis team or auxiliary personnel first collect all relevant information on the incident to get an idea of what happened. It is important when assessing the situation to have as precise a description as possible of the type of incident, its scale, and the sequence of events. Furthermore, information on the measures already taken and on their effect on the situation is also needed.

This information can be obtained by the crisis team itself, taken from the documents available, or obtained from the messages received. Messages can come from trained company personnel, a scouting party, external helpers, or even from the general public. When preparing and creating the messages, it

helps to follow the following basic principles:

- Messages should be brief, clear, and objective, but also complete.
- Messages should contain current information and must therefore be sent immediately. The time of the assessment must be recorded.
- The description of the event should not be over-exaggerated or under-exaggerated.
- The message should clearly state how the event was detected and who detected it, i.e. you observed the event yourself or were told by someone else of the event. The facts should be clearly and explicitly separated from any speculations. It should be easy to discern the source of the message.

The individual messages are relevant to the assessment of the situation. The messages must be evaluated and assessed differently depending on the sender, especially in cases where there are contradictions in the information received. For this reason, the order in which the messages were received and who sent the message must be taken into account when assessing the overall situation.

Depending on type of situation, it may helpful during the assessment of the situation to have some additional information available to assess the situation, for example regarding the terrain and geographic environment, general climatic conditions, or the current level of information possessed by the people affected. To accomplish this, the crisis team needs access to a variety of materials that are usually managed by different organisational units during normal operations. This material includes, for example, architectural building plans, site plans, the rooms currently in use, floor plans, overviews of the supply lines (power, gas, and water), and network plans for the information technology and communication equipment. It must be ensured that the crisis team is provided with the most recent versions of such plans.

Assessment of the situation

Based on the information available, the crisis team makes a mutual assessment of the current situation and of what events could result as a consequence. Possible questions to ask when assessing the situation are therefore:

- What could happen next? What could happen after that?
- What effects could we possibly expect?
- How can the further spreading of damage be prevented?
- How can the damage already done be fixed?

Handling options and specification of measures

Based on the assessment of the situation, possible procedures for managing the specific situation are developed. These options are evaluated in terms of their prospects for success, their advantages are weighed against their disadvantages, their effectiveness is estimated, and any positive, negative, and handling effects that could result from the business continuity measures taken are determined. The idea is to specify a strategy for overcoming the crisis and placing the right resources at the right location and at the right time. When specifying the strategy, the strategic goals of business continuity management and the resources available for responding to the emergency or crisis must be taken into account.

The decisions to use certain handling options, and therefore to take certain measures, are made by consensus in the crisis team. In this case, constructive co-operation is critical to enable the members to come to a consensus quickly. If there are disagreements among the members of the crisis team, then the crisis team leader makes the decision.

One of the first decisions to make in terms of business continuity is which business continuity teams are needed. These teams are then activated. It must be decided, among other issues, which co-ordinated operational plans will be followed, and therefore which specific measures will be taken.

It is also important to decide who to inform in the organisation, and especially who to inform outside

of the organisation. The crisis team, or in case of disagreement, the crisis team leader, decides which measures will be implemented and then issues the corresponding instructions.

Implementing and monitoring measures

The solution developed during the assessment of the situation is divided up into individual tasks. The crisis team issues instructions to the various business continuity teams and auxiliary teams to take those measures that are suitable for eliminating the causes and repairing the damage already done. It monitors the measures to ensure they are taken at the right time.

The effects of the measures taken should be examined regularly and the effectiveness of the measures then evaluated. The current situation is to be re-assessed at regular intervals with the help of the information available, and the latest information is to be used as well when assessing the situation. The re-assessments of the situation must lead to additional measures until the normal state is reached.

Shift operation and shift changes

Crisis management is stressful and is physically and psychologically demanding. For this reason, shifts should be used for those working in the crisis team. A shift should not last longer than 8 hours because the ability to concentrate deteriorates quickly after this time. For this reason, several teams must be used and organisational arrangements must be made for shift operations.

There are basically two different models used to organise shifts: continuous exchange of personnel or a complete change of personnel between shifts. The advantage of the continuous exchange of personnel is that knowledge of the current situation is always available in the crisis team. However, this knowledge must be transferred every time someone is replaced, which then also results in continuous disturbances to the group even though the others can continue to work parallel to the knowledge transfer phase. This makes the advantages and disadvantages of a complete exchange of personnel in shifts clear: one advantage is that there are fewer disturbances since there is only one transfer phase needed per shift change. On the other hand, a lot of background knowledge on the current situation and current management of the crisis is lost each time the shift changes. Another disadvantage is that during a shift change, the entire crisis team or a large part of the crisis team is not available to help overcome the current crisis.

The time required to change shifts should be kept short and should not exceed 15 to 20 minutes per shift change. During this time, all necessary and important information must be exchanged. This includes providing an overview of the current situation, the decisions made, and the measures that have been completed, initiated, or are pending. All members of the team must have the same level of knowledge regarding the current situation after the exchange. Any member of the crisis team with a special task or role must pass his special knowledge of the situation to the person replacing him in this role. To enable a fast transfer of this information, criteria and instructions for guidance should be specified in the conception phase.

De-escalation

Once the organisation has recovered from the emergency or crisis, the situation is de-escalated and the crisis team is formally dissolved (which means its special authorities are revoked). Criteria must be defined for de-escalation just like for escalation. The measures for returning to normal operation are initiated and the normal organisational structure takes over operations.

7.1.5 Business continuity, recovery, and restoration

The most important goal of the business continuity response and crisis management is to maintain business continuity. This means the impaired business processes are somehow put back into operation quickly. Business continuity therefore includes specific measures and procedures that allow the operation of the corresponding business processes to be recovered within the recovery time objective specified in advance. Emergency operation can be obtained by running a “normal operation” using fewer resources, running a reduced operation using alternative resources, or by using alternative operational resources.

If a business process is disrupted, then business continuity can be obtained in the best-case scenario by

recovering the undamaged resources. If resources were destroyed or are not available any more for some other reason, then they must be recovered. Depending on the type of resource, this means that the resource needs to be replaced, re-installed, and set up again.

For the business continuity response, the current situation is analysed and a decision is made for each process regarding which of the business continuity alternatives is possible, reasonable, and the fastest and best alternative in view of the overall situation.

As soon as all recovery and restoration measures have been executed, a message should be sent to the crisis team, regardless of whether or not the measures were successful. The organisation cannot return to normal operations until every point in the restoration plan has been implemented successfully. The organisation remains in the emergency operation phase until this point.

7.1.6 Returning to normal operations and post-emergency tasks

If the resources needed for the normal operation of business processes are available again, then emergency operation should be terminated and normal operation resumed. Since there are dependencies between the business processes that need to be taken into account, the return to normal operations should proceed in an orderly manner to avoid discrepancies between or in the business processes. For this reason, the crisis team must specify the order in which each business process is to be returned to normal operation and at which time, and must also co-ordinate their return to normal operation. This prevents problems from arising while returning to normal operation that could lead to another collapse of the business activities.

In general, there will be work backlogs because emergency operation was performed using fewer resources. To check for backlogs and work off the backlog promptly, one person should be named as responsible in the business continuity plan in each organisational unit for creating an overview of the corresponding work backlogs and specifying a plan to work off these backlogs. When creating the plan to work off the backlog, the currently pending work load, the work load during emergency operations, and the legal work restrictions should be taken into account. Strategic specifications on how to handle the additional time and expense required to work off the backlogs (e.g. using overtime, working in shifts, or using additional personnel) should be specified during contingency planning. These specifications must be agreed to by the personnel representative.

The post-emergency tasks should be supervised by the business continuity co-ordinators of the particular organisational units. It must be specified who will report the status of the post-emergency tasks to whom and at what times.

7.1.7 Analysis of the business continuity response

After completing the business continuity response and de-escalation, the business continuity response should be analysed so that measures for improvement can be taken to counteract any weaknesses discovered. The analysis should be performed by the business continuity officer with the persons responsible from business continuity response, and if necessary in co-operation with the business continuity co-ordinators of the affected areas. Suggestions for improvement are worked out during this analysis.

When responding to an emergency, it may also become apparent that there is a need to improve the organisational structures, the IT, or the business processes. In such cases, the business continuity officer should meet with the people responsible for the particular area and work out suggestions for improvement together. For example, it may make sense to make changes to the fire protection equipment or the information security system.

People must be assigned responsible for the implementation of the suggestions for improvement, and deadlines must be specified for their implementation. The business continuity officer should monitor the timely implementation of the measures for improvement and report to the organisation’s management at prescribed intervals. The plans and procedures used for implementation should be revised and updated by the corresponding organisational units responsible if they are found to be deficient. The functionality and efficiency of the newly implemented measures and procedures should be verified through exercises.

In addition to the suggestions for improvement created when performing the post-emergency tasks, the business continuity response team must create an overall management report. This report must be classified as "confidential" and handed over to management promptly. The report also serves, among other purposes, as the foundation for assessing any eventual legal consequences for or against the organisation or individual persons that could arise from the emergency or crisis.

7.1.8 Documentation during the business continuity response

While responding to an emergency or a crisis, all important actions taken and all decisions made by the crisis team must be recorded in a revision-proof diary for legal reasons. In addition, verification of all incoming and outgoing messages as well as attendance records of the crisis team members should be kept. These records can be provided in electronic or paper form.

The information should be recorded so that the members of the crisis team, but especially the crisis team leader, can quickly obtain an overview of the current situation. The documentation is used to assess the situation, but also, and in particular, when reviewing the emergency or crisis to evaluate and improve the business continuity response processes. It may be necessary to present the financial, legal, and insurance aspects later on as a form of evidence. The following points, among others, must be documented:

- Times at which the crisis team was working
- Situation (type, scope, and flow of events)
- Basic reasons for all decisions made as well as the name and roles of the persons participating in the decision-making process
- Which measures were decided upon, who is responsible for their implementation, deadlines for their implementation, and in particular the implementation status (task supervision)

Standardised forms, for example for verification of incoming and outgoing messages, event diaries, or alarm records can help ensure that the documentation created during the crisis is sufficient and selective. The auxiliary resources required must be worked out and agreed to in advance of a crisis.

The minutes and records are to be signed by the members of the crisis team after completing the response to the emergency or crisis and then stored in a revision-proof manner.

7.2 Psychological aspects of working on the crisis team

Every crisis means enormous mental stress for those involved, but it also represents a complex problem that needs to be solved at the same time. Crises are unique, highly dynamic, and complex events that have numerous variables and parameters. The high degree of networking in modern systems makes it difficult to understand the interaction between the individual parts, the cascading effects, and the side-effects of the decisions made. Wide-ranging decisions need to made under these difficult circumstances that not only can have financial consequences to the organisation, but also can directly or indirectly affect the lives of people.

There are a wide variety of causes of stress in a crisis. Such causes range from shock due to the events, a personal fear of failure; fear for family members; emotional strain; fear of the unknown; sensory overload due to too much information; contradictory or insufficient information; being pressured for time; disruptive environmental conditions such as noise, heat, or cold; hectic actions; or even thirst, hunger, or a lack of sleep. The body reacts to stress just like it did in ancient times by reducing mental capabilities and activating the physical panic reaction. Adrenalin is released, the blood pressure rises, muscles tense up, headaches arise, and heart and circulatory system malfunctions can occur. This can lead to side-effects such as hectic, a lack of concentration, forgetfulness, thinking in circles, blackouts, doing things just for the sake of doing something, inadequate problem analyses, and tunnel vision (which restricts the field of view and changes a person's perceptions). However, reactions ranging from aggressiveness to a complete loss of control can also be caused by stress.

Stress does not only have negative side-effects, but also positive side-effects. Stress can be a driver and motivate people to perform at their very best. For this reason, this factor must also be taken into

account when preparing to work on the crisis team. Crisis team members should therefore possess a certain resistance to stress and should be self-confident. However, it makes sense to take additional preventive precautions. Such precautions include, for example:

- Technical training increases self-confidence and reduces the stress that can arise from insecurities.
- Knowledge of general problem solving strategies and of your own capabilities and patterns of action allow a decision to be made quickly by following an ordered procedure.
- Through training, the members of the crisis team can be prepared for crises to increase their level of stress resistance, to relieve stress using special techniques when necessary, to redirect the stress and put it in a positive light, as well as to refrain from emotionalising the situation. This can be necessary to prevent a spiralling level of stress in which the misjudgements and poor decisions caused by the stress lead to constantly increasing levels of stress, and therefore to more bad decisions.
- Training on the psychological and group-dynamic aspects of working on the crisis team enables more effective co-operation in the crisis team.
- The teams can be prepared to work together in a crisis through exercises. This helps them to develop a common working method and common model of thought. Factors such as the level of trust, development of a common language as the basis for communication in the crisis team, a good working climate, and the ability to judge the other team members to a certain extent can reduce stress.
- External stress factors can be reduced by creating a positive working environment and work conditions (e.g. in terms of food provision, room climate, and resting and sleeping areas).

7.3 Crisis communication

Crisis communication is one of the primary factors for the success of the crisis management. Crisis communication is the communication exchanged with the various interest groups during and after a crisis with the goal of overcoming the crisis, preventing additional damage, providing information, and preventing a lost of image and trust in the organisation. Crisis communication can be classified into internal and external crisis communication. In this document, internal crisis communication is understood to be all communication that serves to respond to the emergency or crisis. The goal of external crisis communication is to provide information. The target groups for this information can be found inside and outside the organisation.

7.3.1 Internal crisis communication

Internal crisis communication includes the reporting, escalation, and triggering of alarms, but also all communication needed to obtain information, co-ordinate the business continuity teams, and co-operate with external locations such as business partners, customers, rescue services, aid organisations, fire departments, the police, or technical emergency services, in order to respond to the crisis.

If the crisis is not restricted to the company or government agency alone, then it may be necessary to inform external locations such as business partners or customers who could also be affected by the crisis. The organisation must also work with these external locations to prevent the damage from spreading. In case the event is a security incident, this can mean talking to the external locations about the possible security problems and possible countermeasures to limit the effects. When this information is not passed on and the locations do not co-operate, the willingness of the external locations to co-operate could be permanently impaired and could seriously affect the level of trust the external locations have in the organisation when they are informed of the security problems through other channels.

In addition to the organisational specifications of who reports, escalates, and issues alarms to whom at what time (see section 7.1.1), and who provides information to whom at what time, the following must also be specified:

- Who is responsible for the individual flows of information between the various parties and roles

when responding to an emergency or a crisis

- When the reports are due and at what intervals
- How the parties will communicate

This includes, for example, the flow of information from the site of damage or from the business continuity team to the crisis team and back. Special attention should be paid in this case to the technical and logistical aspects of crisis communication. When examining these aspects, answers to the following questions, among others, must be developed:

- What form do the communication processes needed to respond to the emergency have (verbally, as text, data, video, or pictures)?
- Which communication systems (end devices and connections) are available at the various locations and what are their alternatives?
- What is the risk of failure of each of the communication solutions?
- Which measures must be taken to ensure the availability of the communication systems needed in an emergency?

Secure and reliable communication is needed in a crisis, which means a high level of availability of the communication systems must be guaranteed in a crisis. Possible preventive measures include having a sufficient number of end devices, a secure power supply for the end devices, and especially the provision of alternative lines of communication (e.g. using the Internet, land lines, mobile communication means, satellite communication). However, the confidentiality and integrity of the communication and the authenticity of the communication partner should also be taken into account when selecting the systems.

7.3.2 External crisis communication

Every crisis is also a communication crisis since the detection of the crisis, the response to the crisis, and the response of management in the public eye are deciding factors. The public also takes part in deciding on the scale of the crisis. The goals are to prevent gossip, channel emotions, and reduce or prevent fear. For this reason, it is essential to specify clear responsibilities and a strategy for external crisis communication, which is also referred to as crisis PR (public relations).

Organisational structures

The crisis communication leader in the crisis team is solely responsible for external crisis communication. All contact with the media should be made by this person alone or co-ordinated by this person. This person can be provided with support by other employees who take on and perform special tasks such as contacting the media, holding press conferences, or editing the online information. It is helpful to have the following roles in the crisis communication team: a crisis spokesperson to provide the public with information, a technical expert to answer scientific and technical questions, a legal expert for legal questions, and an expert in press and public relations who is then responsible for monitoring the media.

The members of the external crisis communication team should be prepared for these tasks through appropriate, regular training or education programs (e.g. media training) so that they can react accordingly to unforeseen questions and handle the extreme stress and pressure for time. They must learn not to be provoked into providing rash statements and to retain their composure. The idea is to place critical questions to the members, in many cases regarding their own failures, and ensure they never react aggressively. Crisis communication is a demanding and complex task. Specialists are needed to perform these tasks professionally. Training programs of this type are run by agencies specialised in crisis communication, among other organisations.

If there are not enough internal resources available, then it must be determined if it makes sense to utilise an external crises communication expert in a crisis. This expert should be selected in advance, be required to sign a contract, and familiarised with the organisation and the terminology it uses.

It must be ensured that the crisis communication leader has enough information available during the

crisis regarding the possible damages, the countermeasures taken as well as those planned (without any details), and on which locations have already been informed. He checks and approves all information on the crisis which will be disclosed for the purpose of providing information. If a representative from management is entrusted with subtasks relating to crisis communication, for example with maintaining contact with important interest groups, then this person's tasks and authorities must be specified clearly to prevent any misunderstandings.

Communication strategy

A communication strategy and lines of communication that guarantee consistent informational content and consistent argumentation in a crisis must be clearly specified. The crisis communication strategy defines the framework and basic principles for communication as well as the terminology and phrases to be used. It specifies who collects the information for crisis communication; which target groups will receive which information at what time, in what detail, and over which paths of communication or media it will be distributed during a crisis. The details of this strategy must be specified a crisis communication plan.

In a crisis, it helps to identify the relevant interest groups, their requirements, values, goals, and possible interest in the information when developing a crisis communication strategy. The analysis of the interest groups performed during the initiation of business continuity management can be used as a starting point to identify the interest groups. In addition to the interest groups already mentioned, such as the owners, investors, management, employees, suppliers, and customers, there are also other interest groups that play an important role in crisis communication.

These groups include, for example, family members, neighbours, the general public who is not directly affected, regulatory authorities, political representatives, competitors, environmental groups, public action groups, protesters, and especially the various media. The groups can be classified into internal groups of the organisation, directly or indirectly affected external groups, and other interest groups (see Figure 12).

Figure 12: Target groups of crisis communication

The goal of the analysis is to identify the different interests for information on the crisis and the motives of the groups, and then to develop strategies and measures for dealing with these groups. It makes sense when conducting the analysis to include the influence of each of the various interest groups and their sanctioning capabilities (e.g. protests, boycotts, legal steps) as well as the possible implications to the organisation to be expected. The level of information and knowledge available to the particular target group also plays an important role when preparing the information for each group.

Basic principles

Several basic principles should be observed for external crisis communication and when specifying the communication strategy:

- Every large-scale crisis in an organisation will become public sooner or later. For this reason, it is

necessary or at least advisable to inform the public promptly. After carefull consideration the media should be contacted at an early stage which makes it possible for the organisation to influence the public's perception of the crisis and of the crisis management in the organisation's favour wherever possible. As the German saying goes, "He who is silent is in the wrong".

- Even if the public external groups are not informed of the full scale or of all details, the statements issued during the crisis communication must still be true.
- The communication should be factual, but should also express a certain degree of empathy and sympathy. The information communicated must be appropriate for the situation.
- Avoid making conjectures and speculations.
- Do not conceal any piece of news, not even bad news, because information can only be concealed for a short time nowadays. Half-truths, concealed information, subdued or forced retractions create defensive attitudes.
- The information communicated should present the events in a simple manner, but without adulteration, because incomprehension creates fear.
- The information provided to the public should be made abstract enough so that it does not encourage imitators and competitors cannot derive any advantages from it.

Information paths

A central location, e.g. a central hotline, should be set up to receive and reply to all external questions according to specific guidelines. Support can be provided to this location by the corporate or governmental communication organisational unit, public relation department, or press office. This location should have permanent telephone and fax numbers and email addresses, which must also be made public in a suitable manner. Consideration should be given to setting up a free telephone crises hotline. Depending on the size of the organisation, the industry in which it operates, and the expected crises, it may make sense to contract a specialised professional provider (e.g. a call centre) to handle the flood of questions coming in during a crisis situation. Note though, that this provider should be selected in advance, bound accordingly by contract, and have been trained in crisis communication. A central point of contact should be named for the employees and their families where they can obtain additional information. It is important for all points of contact to examine the identity of all persons requesting information on the incident or the situation.

In addition to setting up points contact to provide information on request, paths should also be prepared to pro-actively distribute information on the crisis and the organisation's response to the crisis. Such paths include the Internet, but also contacts to journalists or press conferences. Media representatives work in a highly competitive field. They all want to publish the best story; one that focuses on the human factor and generates emotions. For this reason, the goal should be to channel the media representatives and the rush of people at the site. The media representatives should be informed as quickly as possible, kept up to date at all times, and supplied with information. Contact data is needed to contact the media directly, and this data must be acquired in advance and maintained. It helps to set up a network of contacts to the local, regional, or even national media, and maintain personal contacts to journalists and trade media that will stand up under stress.

User-friendly online pages can also have a widespread effect. Informational pages published in the Internet that are prepared in advance and then adapted to the particular crisis can provide information on the current status, for example. To be able to react quickly, the crisis information pages, which are to be prepared in advance as dark sites for the web server of the organisation so that technical personnel are not needed in a crisis to create the web pages. If special pages for specific target groups are published, for example in the Intranet for employees or in the Internet for their families or the media, then it must be ensured that these pages can only be accessed with the proper authorisation.

Aids and technology

To ensure fast and appropriate communication, templates, pre-defined explanations, and text fragments should be created in advance for the situations expected. Even specially prepared and selected background material can be useful so that the media can be supplied with individual press

folders adapted to the specific situation. When communicating in a crisis, the following rule applies: Never get defensive.

Suitable, functioning communication resources are needed for a crisis. These resources, as well as the technology and the rooms for press conferences, are to be planned and prepared accordingly in the contingency planning phase.

Detailed information on external crisis communication, especially for government agencies, can be found in [BMIKK].

7.4 Business continuity handbook

The business continuity handbook contains all documents required for business continuity response and summarises the structures, information, measures, and actions necessary to handle an emergency and recover business operations.

It must be prepared in advance together with the contingency planning concept, and must also be adapted to the contingency planning concept. The main part of the business continuity handbook is the plan for the immediate measures, the crisis team guide, the crisis communication plan, the business continuity plans, and the recovery plans. Depending on size and complexity of the organisation, this information may be contained in one or more documents. A small or medium-sized organisation can collect all the information needed in an emergency in one document. For large organisations, it is recommended to distribute this information among several documents. These documents must be co-ordinated to reflect the same information in order to avoid conflicts and a guarantee the various groups act accordingly in a crisis. To ensure a uniform structure and manageability of the documents, a common document template and format should be created for each of the various types of documents contained in the business continuity handbook.

The purpose of an business continuity handbook is to provide a documented procedure and additional help so that the organisation can manage the emergency or crisis and ensure the continuity of their critical business processes. The business continuity handbook should be organised so that it provides fast and simple instructions.

There are several ways to organise a business continuity handbook:

- Organised by phases that reflect the chronological sequence of actions when responding to an emergency
- Organised by levels or areas of responsibility and/or by roles which are based on the various tasks to be performed
- Organised by process, whereby specific business processes or groups of processes are targeted

Which structure and modularisation is most useful for an organisation depends on its size and structure. Any combination of these possibilities can be used, but the same basic principles should be taken into account in this case:

- Information that changes often should be collected at a central location in the business continuity documentation so that it is easier to update this information.
- A modular structure should guarantee that the employees responsible can quickly find the section relevant to them or that this part can be taken out and handed to them.
- It must be ensured that the business continuity documentation is concise and always up to date so that the measures necessary in an emergency can be implemented quickly and no important tasks are forgotten in the stressful situation of an emergency.

A sample table of contents for a business continuity handbook can be found in Appendix C. Note though, that an business continuity plan must be specially adapted to the particular organisation, its organisational structure, and its requirements in terms of business continuity, and it is therefore impossible to provide a generally applicable template. The sample template is only intended as an initial starting point.

7.4.1 Immediate measures plan

The first steps when responding to an emergency or a crisis are to guarantee the security and safety of people. For this reason, all immediate measures such as the rescue or evacuation of people must be collected in a corresponding plan.

7.4.2 Crisis team guide

The crisis team guide, which is also sometimes referred to as the crisis management guide or crisis management handbook, specifies objectives, basic principles, and general conditions for the strategic and tactic actions taken in crises of all types. The crisis team guide primarily covers crises for which no action plans are available due to their uniqueness or unforeseeability. This especially includes crises that are not the result of damaging events and do not impair business continuity. The target group of the guide is therefore the crisis team of the organisation-wide crisis management.

For these reasons, this subplan should be developed in the framework of the organisation-wide crisis management, or should at least be adapted to reflect the crisis management policies.

The crisis team guide offers, among other things, aids in the area of emergency or crisis response as described in this document for assessing the situation and for selecting suitable subplans and options for business continuity. The idea is to protect the interests of the various interest groups. The crisis team guide contains additional basic information regarding the organisational structure (roles, tasks, and rights), the operational structure, and the contact persons with contact information, but especially the persons and companies who are fundamentally important when responding to a crisis.

7.4.3 Crisis communication plan

The crisis communication plan regulates how internal and external communication should be performed in a crisis (see section 7.3). This includes communication with the employees and their families, with the most important interest groups, and especially with the public and the media. The crisis communication plan specifies, among other things, who is allowed to pass what information to whom and how this information is to be passed. The crisis communication plan can also be part of the crisis team guide.

7.4.4 Business continuity plans

The business continuity plans summarise the reactions of the organisation to a disruption in business after a damage event at the process level. It is used to analyse the situation and develop suitable strategies for the quick recovery of the critical business processes. It has been shown in practical applications that it is best to develop a separate business continuity plan for each logical organisational unit. The purpose of the business continuity plan is to provide a documented procedure that can be used to resume operation of the critical business processes within the specified recovery time objectives. It contains a description of the emergency operation method, i.e. if the original location or an alternative location will be used, or if the standard process or an alternative process running at a reduced capacity will be used.

The business continuity plans for the individual organisational units are to be consolidated, and they must be co-ordinated in terms of their contents, schedules, and personnel. Together they form the overall business continuity plan.

A business continuity plan should contain the following points at a minimum:

- The scope
- A presentation of the continuity strategies and process options for various damage scenarios
- A list of responsibilities
- A list of the business continuity teams with contact information
- Criteria for activating and deactivating the plan

- The alarming and escalation procedures for these teams
- An overview of the recovery requirements for the business processes
- The process priorities
- Instructions for co-ordinating the post-emergency tasks

The business continuity plan should contain the following information at a minimum for each of the processes:

- Measures for fast activation of business continuity
- Process descriptions for emergency operation or the various alternatives (e.g. using alternative resources available internally or starting an alternative process), including any necessary aids
- Descriptions of the roles
- Measures for returning operations to the normal state
- Measures for the post-emergency tasks required

The business processes are to be listed in order according to the priority specified. The procedures and measures described in the plans should guarantee the performance requirements defined during the BIA for the continuity of the critical business processes.

A sample table of contents for a business continuity plan can be found in Appendix D.

7.4.5 Recovery plans

The recovery plans contain the specific instructions and information necessary to recover and restore resources. They therefore supplement the business continuity plans and serve as a working basis for the corresponding business continuity teams.

The recovery plans contain information for individual resources as well as overall plans that cover the simultaneous failure of several systems. An example of such a situation is the failure of a computer centre. The corresponding overall recovery plan could contain instructions for switching to an alternate computer centre and putting it into operation.

The recovery plans should also contain an overview of the resource priorities, and therefore the order in which they are recovered. The following information should be recorded for each resource, among other information:

- The criticality
- Recovery time objective and, if necessary, any special time periods
- The interfaces and dependent resources
- A short description of the resource
- Measures for eliminating errors, recovery, restoration, emergency operation, and returning to normal operation
- The contact persons, e.g. the specialists responsible for the business processes

8 Tests and exercises

To ensure the appropriateness, efficiency, and currency of the contingency plan and of the response to an emergency or a crisis, the preventive measures, organisational structures, and various plans must be checked regularly in tests and exercises.

Tests and exercises verify the assumptions on which the concept is based. The implementations of individual measures or bundles of measures are checked for correctness, and the operability of the technology is tested. Exercises also demonstrate if the business continuity documentation is useful and if those involved are also able to perform the tasks assigned to them in an emergency.

Exercises train the procedures described in the plans, enable personnel to perform the required actions routinely, and verify the efficient function of the solutions. They improve the reaction time and provide the employees with a sense of security when taking action. Since people in crisis situations tend to react without thinking, hastily, incorrectly, and irrationally in particular due to the associated stress, the exercise goals stated above should not be underestimated.

Tests and exercises come in conjunction with time and expense. To ensure the investment in testing and exercises is used reasonably, the investments need to be planned. For this reason, an exercise concept and an exercise plan should be created. The plan should take different types of tests and exercises into account. Some examples are described in the following sections. The types of tests and exercise selected depend on the type and size of the organisation as well as the local environment, and they must therefore be selected on a case-by-case basis.

8.1 Types of tests and exercises

Some types of tests and exercises are presented in the following. The types range from the simple examination of individual measures to complex business continuity exercises. Simple examinations are often referred to in this document as tests, while more complex examinations of specific scenarios are referred to as exercises. Note, though, that it is impossible to strictly separate these terms. Many statements apply to both types of examinations.

Testing the technical preventive measures

To ensure the appropriateness and operability of the technical solutions, these solutions need to be tested. This includes, for example, tests of redundant lines, the power supply, the restoration of data from data backups, the reliability of clusters, the alarm technology used, the technical infrastructure, or individual IT components. Individual components and their function should be tested regularly and after making large changes to the systems or the corresponding system environment to check their interoperation.

Function test

In this type of exercise, the functionality of the procedures, subprocesses, and system groups specified in the various subplans of the business continuity handbook are examined. During the examination, the procedures, but especially the interoperation and dependencies of the various components or measures, are checked. This includes recovery plans, restoration plans, and the business continuity plans for immediate measures (e.g. for evacuating the personnel in case of a fire alarm).

Plan review

The goal of a plan review is to examine the individual plans for emergency or crisis response. The participants go through the plans theoretically in this type of test and examine the plausibility of their contents and the assumptions made in them. The functionality of the contents described is evaluated at that time.

Tabletop exercise

The term tabletop exercise is used to refer to the theoretical examination of problems and scenarios

"on a table" – which is why it is called a tabletop exercise. In this type of exercise, a hypothetical scenario is given and then examined theoretically. This type of test is relatively easy to implement and is used for initial validation. Discrepancies and misunderstandings can be detected using this test before expensive and time-consuming operative efforts are required. This type of test should be repeated often during the business continuity management establishment phase.

Crisis team exercise

A special form of tabletop exercise is the crisis team exercise. In this case, the exercise is performed in co-operation with the crisis team.

Command post exercise

Another form of tabletop exercise is the command post exercises, which is basically an enhanced version of a crisis team exercise. It is used to examine and practice co-operation in the crisis team as well as to examine the level of co-operation between the crisis team and the operative teams. In general, the structures close to the command post are tested in practical exercises while the operative implementation is simulated theoretically.

Communication and alarm exercise

A critical point when responding to an emergency or a crisis is the reporting to and alarming of the crisis team and other people responsible. For this reason, the procedures for reporting, escalating, and alarming must be examined regularly. The scope of this test ranges from simple examinations of the communication resources to the assembly of the crisis team in the crisis team meeting room. In this test, the responsibilities and telephone numbers contained in the plans as well as the procedures, escalation strategy, ability to reach the corresponding people, and rules for substitutes are tested. The test also checks if the plans available are up to date, understandable, and manageable; if the procedures are practical; and if the technologies to be used (e.g. alarm system, emergency telephone, SMS, pager, Internet, radio or satellite communication device) are effective, appropriate, and ready for operation.

Simulation of scenarios

In a realistic simulation, the procedures and measures specified for responding to business continuity scenarios or events are tested in terms of their usefulness, appropriateness, and functionality. In this simulation, the alarming, escalation, business continuity response organisation, work done by the crisis team, and level of co-operation between all participating locations is tested. Such exercises can be organised as function or area tests, and in a further stage, they can be organised to cover all areas.

Business continuity or full scale exercise

The most complex type of simulation is the business continuity or full scale exercise. Depending on the scenario, it is necessary to include external organisations, for example the fire department, aid organisations, government agencies etc., in the exercise. This type following exercise can and should only be performed in the advanced stages.

The full scale exercise is based on a realistic situation and integrates all levels of the hierarchy, from management down to the individual employees, into the exercise. The time and expense required for preparation, execution, and evaluation should not be underestimated. In spite of this, full scale exercises should be conducted if the organisation places high requirements on business continuity management. Business continuity exercises should be performed regularly but with longer intervals between each business continuity exercise.

Comparison of the different types of exercises

Various criteria can be used to differentiate between the different types of tests and exercises. They can be classified according to the type of procedures, target group, scope, or extent.

The procedure followed can be based on discussions or actions. There are three areas of responsibility for the target groups: the strategic, tactical, and operative areas. Exercises at the tactical level examine the co-ordination, the level of co-operation between the individual areas, and the procedures for

assessing and evaluating the situation. At the operative level, the focus is on the procedures and the specific tasks to be performed to overcome the emergency (see Table 18).

Exercise type	Target group			Procedure		Extent/ scope
	Strategic	Tactical	Operative	Discussion -based	Action- based	Low/ Medium/ High/ Very high
Test of the technical preventive measures			X		X	Low
Function test			X		X	Medium
Plan review		X	X	X		Low
Tabletop exercise		X	X	X		Low-medium
Crisis team exercise	X	X		X		Low-medium
Command post exercise	X	X	X	X	X	Medium-high
Communication and alarm exercise		X	X		X	Low
Simulation of scenarios		X	X		X	High
Business continuity or full scale exercise	X	X	X		X	Very high

Table 18: Types of exercises

8.2 Documents

It is helpful to create various types of documents for planning and performing exercises and tests: the exercise concept, the exercise plan, the exercise manual, and the exercise minutes.

8.2.1 Exercise manual

All business continuity management tests and exercises in an organisation need to be planned and prepared. For this reason and to keep the number of disruptions to actual operations as low as possible, strategic decisions, basic specifications, general conditions, and agreements on all tests and exercises to be performed must be made together with the organisation's management. These are then collected in the exercise manual and form the foundation for planning general exercises and individual exercises.

The exercise manual should answer the following questions, among others:

- What is the strategic importance of the business continuity tests and exercises to the organisation?
- What are the goals to be reached by performing the tests and exercises?
- How much value does the organisation place on performing the tests and exercises?
- Into which types does the organisation classify the tests? How much time is involved for each of these types and what are the rough costs associated with each type?
- What are the goals of each type of exercise in the organisation?
- How many tests and exercises should be performed? Are there legal or supervisory regulations regarding the frequency of the tests and exercises?

- Which roles will be defined when planning and performing tests and exercises? Which tasks, rights, and responsibilities do these roles have?
- Which areas should be tested: the knowledge and capabilities of the participants and employees, the business continuity management procedures, the mechanisms and technologies used, the business continuity documentation, the operability of central resources, the measures planned, etc.?
- Which exercise methods will be used (e.g. announced or unannounced)?
- How will the interface to the operative daily business for performing exercises be defined? To what degree is the exercise allowed to influence daily business operations, provided that it is even allowed to influence daily operations at all?
- How will the tests and exercises be documented? What level of detail will be documented?
- How will the results of the exercise be assessed?

The exercise manual contains the strategic basic principles as well as helpful aids for detailed planning, performing and evaluating exercises and tests. This includes, for example, document templates for invitations, announcements, log records, or evaluation questionnaires that need to be filled out for or adapted to specific exercises.

8.2.2 Exercise plan

It makes sense not only to examine the next exercise to be performed, but also to plan a series of matching tests and exercises that, as a series, cover all areas of the organisation as well as all parts of the business continuity plans to be tested. For this reason, the intervals, order, and the basic, general data of the planned tests and exercises are specified in the exercise planning phase for a period spanning a few years. In the exercise planning phase, all types of tests and exercises, from simple system tests to the simulation of scenarios, should be planned at a minimum. It is not enough just to test individual contingency measures in the framework of change management.

When specifying the dates for the tests and exercises, general conditions such as holiday periods in which the employees are unavailable or special time periods for the organisation and business processes must be taken into account. When specifying the order of the tests and exercises, keep in mind that experience has shown it is best to place them in order from the simplest to the most complex. Tests not requiring much preparation should be performed more frequently. The frequency and scope of the exercises should be based on the threat scenario applying to the corresponding organisational unit. A risk-based approach is recommended. The more critical a process or system is to business continuity, the more frequently the contingency measures and plans need to be tested.

Experience has shown that tests and simple exercises should be performed annually. For example, at least one exercise should be performed each year, for example a building evacuation exercise. Organisations with high availability requirements on the business processes should perform extensive business continuity exercises, for example moving into an alternate site and testing the functionality of the emergency workplaces, at least once every 2 to 3 years. Depending on the industry in which the organisation operates, there may be legal or supervisory regulations regarding the type, number, or frequency of the exercises that need to be observed.

In the exercise plan, the planned scenario, the type of exercise, the purpose, the goals to be achieved, whether the exercise is announced or unannounced, the planned participants (roles), and the time and expected duration of the corresponding exercise must be specified for each test and each exercise. A rough estimate of the personnel requirements and of the material and financial resources should also be made.

The plan should be co-ordinated with the personnel representative and with the organisation’s management, who then approve the plan.

8.2.3 Test and exercise concept

A separate test or exercise concept must be worked out for each test and exercise. This concept

contains the detailed execution plan. A test concept describes which method is used to test a system, which tools will be used, and what general conditions are prescribed. An exercise concept describes the group of participants, the role each participant assumes in the exercise, the chronological framework, and the criteria for terminating the exercise. It therefore contains the following specifications at a minimum:

- Name of the exercise
- Time, date, and planned duration of the exercise
- Location of the exercise
- Type of exercise
- Goals
- Exercise leaders
- Participants, observers, record keepers
- Instruction of the participants (the briefing)
- Scenario

An exercise concept should be created in two stages. First, a basic concept is created and submitted to management for approval. After that, the detailed concept is created. The following additional points should be taken into account for longer, large-scale exercises such as emergency and full scale exercises. This includes, for example, taking security precautions during the exercise to protect the participants or supplying them with food and beverages.

Exercise script

An exercise script must be created for more extensive exercise scenarios. In this script, the initial situation, the specific sequence of events in the exercise, the predefined events, and the order in which these events occur are to be described in as much detail as possible. It must also be specified how the corresponding particular information will be transferred to the participants and by whom. The script helps the moderators of the exercise to specify the sequence of events during the exercise.

The scenario technique is usually used as the method for developing an exercise script. In this method, the realistic paths of development of the situation are pointed out to the organisation based on a hypothetical damage event. To avoid the participants from becoming accustomed to the exercises and to re-motivate them, each exercise scenario, and therefore the exercise itself, must be designed to be unique.

The initial situation is documented in the “blue situation”. This documentation serves to provide the exercise participants with information on the current situation at the beginning of the exercise. It contains a description of the normal situation, the occurrence of a damage event, all necessary information on the current situation, and ends with the “task” corresponding to a real alarm. The term “blue situation” is used due to the fact that all written documentation on initial situation of the exercise is usually printed on blue paper so that it cannot be confused with other documents.

One way of formatting an exercise script is using a table. In this table, a sequential number is placed next to each individual activity (also referred to as a single situation), and the time, a short description of the event, the goals of the test, the expected reaction, the players, and any tools or aids used are specified for the single situation (see Table 19).

Exercise: XYZ											
No.	**Real-time**	**Scenario-**	**Keyword**	**Activity**	**Goal / reaction expected**	**Person taking action**	**Players**				**Aids/ tools/ type of action**
							A	**B**	**C**	**…**	
1	…		…		…		…	…	…	…	…
2	10:10		Report to Alarm Centre	(Description of the single situation with background information)	Examination of the alarm, escalation	Mr. Jansen		X	X		Mobile phone
3	…		…	…	…		…	…	…	…	…

Table 19: Example of an exercise script

8.2.4 Test and exercise minutes

The execution and the sequence of events in tests and exercises are to be documented carefully in test or exercise minutes. These minutes contain information on which time schedule was used as the basis, how the participants proceeded during execution, which methods were used, which tools were used with which configurations, and which results were obtained. In particular, any problems arising or deviations from the test, exercise schedule, or the expected goals found should be recorded. The test or exercise minutes form the basis for the assessment performed after the test or exercise, the determination of the weaknesses, and any suggestions for improvement.

8.3 Performing tests and exercises

8.3.1 Basic principles

Some basic principles must be followed when performing tests and exercises. For example, the tests or exercises should not or only minimally disrupt normal operations. When selecting the time and date of execution, it must be taken into account that a test or exercise could have a direct influence on operations, among other things. The systems to be tested may only be available at a lower level of performance for productive operations during a test or may not be available at all. For this reason, it is usually recommended to perform tests and exercises outside of regular business hours, if possible, to minimise the effects on live business operations.

The employees involved in the exercise must leave their daily work behind during the exercise phase. The time they are involved in the exercise must be considered work time and credited to their work accounts. If tests and exercises are performed outside of regular working hours, then the corresponding agreements must be made with the personnel representative.

Measures must be planned that ensure that the exercise remains under the control of those involved and does not itself lead to any malfunctions. Termination criteria must be specified as well as fallback solutions to enable the fastest possible return to normal business operations must be planned in case unexpected malfunctions arise due to the exercise. Possible termination criteria for an exercise could include the expiration of a certain time or the recognition that the measures implemented cannot be used to achieve the desired success.

8.3.2 Roles

Extensive work is required for the planning, preparation, and execution of exercises. For this reason, the roles for preparing and executing the exercise must be specified together with their tasks and rights.

Exercise author

An exercise author should be appointed to prepare the exercise. This persons job consists of developing the exercise plan as well as designing the individual exercises, from specification of the scenarios and selection of the participants to the preparation of the environment in which the exercise will be performed. These tasks should not be underestimated and require more or less time, depending on the type of exercise to be performed. The exercise author should be very familiar with the contingency planning concept as well as with the individual emergency, recovery, and restoration plans. This role can also be assumed by the business continuity officer or the leader of the crisis team.

Preparation team

To create and develop exercise concepts and exercise scripts, the exercise author needs the help of a preparation team. The preparation team can include heads of organisational units or the persons responsible for processes, whose expert knowledge can then be used.

Exercise manager / moderator

The central role when performing an exercise is the role of exercise manager or moderator. This person's tasks include, among others, initiating the exercise, co-ordinating the individual activities, making decisions on alternatives or deviations from the plan, and declaring the exercise to be officially terminated.

Core team

The exercise manager is supported by the command post leaders. The core team's tasks consist of providing technical consulting, answering questions from the exercise participants, or introducing single situations to illustrate the situation in the exercise scene. In addition, the core team also includes one or more keepers of the minutes, the exercise author, the business continuity officer, and, if necessary, observers of the core team.

Keeper of the minutes

A keeper of the minutes has the important job of recording a detailed sequence of events during the exercise. Depending on the scope of the exercise, number of sites involved, interest groups represented, and other factors, it may also be necessary to use several keepers of the minutes who observe and record the situation from different perspectives.

Observers

Other observers can also be allowed to observe the exercise in addition to the keepers of the minutes. Observes can include, for example, members of the internal audit department, but can also include employees from other areas, external experts, or representatives from government agencies or aid organisations. They are neutral observers while the exercise is underway and do not intervene during the exercise. However, this group should also be involved in the assessment of the exercise by requesting their observations and assessments as well.

Players

The group of players can include the person responsible for the process, persons responsible from the organisational units, representatives of the employees and management, but also customers, service providers, suppliers, or other external parties. However, the inclusion of external parties should be avoided in the group of players if the business continuity management system is still being established.

8.3.3 Procedure

The execution of an exercise can basically be divided into four phases:

Planning and release

The execution of a test or an exercise must be planned like a project. This includes scheduling and personnel planning for the entire process, from the conception of the exercise to the post-exercise tasks. The scenario is worked out and the documents needed to perform the exercise are created in this phase.

The exercise concept must be approved and released by the organisation's management. Approval and release can be done after planning, but it may make sense to have a rough draft of the exercise concept approved to prevent time-consuming misplanning.

Preparation

The conditions for the exercise are created in the immediate preparation phase. This includes, for example, configuration of the environment and any necessary preventive or security safeguards such as making an additional data backup, preparation of replacement systems, or informing rescue services, government agencies, or the local press to prevent false alarms due to misunderstandings. The resources for the exercises must be provided according to the recovery plans.

Depending on the level of knowledge of the participants, it is generally recommended to inform them that an exercise will be performed, why it will be performed, which safeguards are necessary, and of the flow of events for the exercise. The exercise meeting, also referred to as the briefing, is held shortly before the actual exercise. In this briefing, the current roles are illustrated, the schedule is presented, and the contact person and telephone lists are made available, among other tasks. Depending on the type and goals of the exercise, not all participants may need to be fully informed. Who will receive what information on the exercise procedure in advance must be specified when planning the exercise.

Execution

An exercise is started at a predefined time by the exercise manager. The exercise manager co-ordinates the exercise and decides if and how deviations from the plan will be handled.

The players should be guided by the exercise manager to prevent the exercise from drifting into chaos, but without hindering their creativity too much. To keep the exercises going without stopping, the activities specified in the exercise script are initiated by the corresponding players.

The keepers of the minutes take the exercise minutes. The exercise minutes should document the course of the exercise, the goals reached, and the problems encountered by the exercise participants while performing the exercise activities. Each entry should contain what has been observed, the time and date the entry was made, and the name(s) of the observer(s). The exercise minutes are used later as the basis for the evaluation of the exercise, which is done later. The minutes also serve as verification of the execution of the exercise for internal or external audits.

Every exercise should be terminated officially by the exercise manager. The environment created for the exercise (if one was created), must then be returned to its normal state. For exercises covering more than one site, the corresponding documents and minutes must be collected at a central location.

After the end of the exercise, a short closing meeting should be held together with all participants. In the closing meeting, the course of events during the exercise are summarised and, if necessary, a preliminary evaluation of the exercise is made.

Evaluation

The exercise should be evaluated by a predefined group selected from the participants. During the evaluation, the results are compared to the specified goals and the course of events recorded is analysed for weaknesses.

The goal of the evaluation is to identify potential improvements to the contingency plan and the

business continuity response, but also for carrying out exercises. The evaluation is based on the exercise minutes, but also on the evaluations of the exercise participants and observers.

The evaluation of the exercise is to be documented. The exercise manager creates a final report on the exercise performed together with its results, and then submits this report to the organisation's management.

Responsibilities and measures for eliminating the deficiencies detected as well as implementation deadlines for the corresponding measures must be specified. The implementation of the measures is to be checked by the business continuity officer. The effectiveness of the measures should be checked again no later than the time of the next exercise.

9 Maintenance and continuous improvement

To enable the maintenance and continuous improvement of the business continuity management process, it is not only necessary to implement appropriate preventive measures and update documents continuously, but also necessary to test the business continuity management process itself regularly in terms of its effectiveness and efficiency. In this case, regular checks and evaluations of the process must be performed by management (management evaluation). All results and decisions must be documented so that the decision can be understood later.

9.1 Maintenance

To maintain the effectiveness of the business continuity management process and the contingency measures implemented, the process must be monitored, controlled, and updated continuously. Monitoring permits the early detection of potential improvements in the business continuity management process. Suitable measurement and evaluation criteria should be developed for each organisation as the basis for monitoring. The values of these measurement parameters must be measured regularly, and the development of the values must be observed. If the values develop negatively, then the causes should be determined, measures for improvement should be defined, people should be named responsible for their implementation, and appropriate changes should be made. The results should be prepared in the form of a report, which is then submitted to the organisation's management for the purpose of raising awareness. The business continuity officer is responsible for the performing the steps described here.

Examples of suitable measurement and evaluation criteria include:

- The number of exercises performed (successfully/unsuccessfully)
- The number of tests conducted (successfully/unsuccessfully)
- The number of emergencies that occurred (and how many were managed successfully)
- The number of training programs held (number of participants/number of hours)
- Time needed to alarm the crisis team
- The number of risks whose threat was reduced compared to the total number of risks

In addition to monitoring and controlling the business continuity management process, the currency of the measures, and in particular of the documents, also play a decisive role. To keep them up to date, it is necessary to specify change triggers in various business processes. The triggers should activate when changes arise in the following areas:

- In the strategic direction of the organisation, the business fields, or the priorities of the interest groups
- In the general conditions, i.e. legal conditions or other such conditions
- In the environment, i.e. the location of the organisation or relocations within the organisation (e.g. of emergency workplaces)
- In the business processes
- In personnel
- In the technology used
- When a new software release is available for a system, provided that this system is part of the contingency planning concept.

The corresponding part of the business continuity management process must be examined for such changes. If necessary, change measures must be triggered by the change management.

9.2 Examinations

The ability of the organisation to handle emergencies and crises can only be determined through regular examination of the business continuity management process and the contingency measures. The goal of such examinations is to ensure the operability, effectiveness, appropriateness, and efficiency of the business continuity management process. To do this, deficiencies as well as potential improvements are pointed out, and recommendations are provided.

The examination of the business continuity management process should be performed at different levels. Self-assessments, in which the business continuity officer and the business continuity co-ordinators examine (themselves or by others) the correct implementation of their specifications, the current coverage, the efficiency, and the maturity of the business continuity management process form the innermost level. This examination checks, among other things, if the implementation of the measures was performed correctly and according to the specifications, how many of the specifications were implemented, and if the specified processes are actively supported.

In the next stage, independent audits are performed by the independent internal audit department according to the recognised basic principles of the auditing profession. The organisation's management must request the internal audits to be performed. When performing internal audits, the auditor must document if the management is fulfilling its auditing duties, among other things. The auditor should be competent and independent, and the auditor's competence and independence must also be examined, if necessary. In an internal audit, special emphasis is placed on the checking if the internal and external guidelines are being followed and on comparing the process to standards and best practices (compliance). However, the effectiveness and appropriateness of the business continuity management processes must also be examined.

The internal audits of the business continuity management process should be planned based on a risk-oriented approach and must be co-ordinated with the organisation's management. The audit plan specifies the goals, the type, the scope, and the content of the audit as well as the roles to be filled when performing the audits. When performing an audit, all relevant observations must be documented by the auditors and then evaluated in a post-audit evaluation. Examples of possible auditing methods to be used include, for example, document examinations, interviews, and inspections. The results are to be written in an audit report containing the observations made by the auditors and what actions are required. The audit report is to be submitted to the business continuity officer and the organisation's management.

External audits are initiated by outside monitoring agencies. External auditing or consulting companies are usually contracted to perform external audits. The methods and procedures for audits are regulated by specifications and standards from the professional associations, for example from the IDW (the German Institute of Auditors). In government agencies, external audits are usually performed by auditing offices.

The regular examinations of the business continuity management processes performed in the various stages must be planned, executed, and the results documented. The problems detected during an examination must be eliminated as quickly as possible. For this reason, the necessary corrective measures are to be developed by the business continuity officer and specified in the form of an implementation plan. This plan contains a schedule, resource plan, assignments of responsibilities, as well as specifications for the examination of the implementation status. The business continuity officer is also responsible for the implementation of the corrective measures and ensuring the required resources are used properly.

9.3 Flow of information and management evaluation

In order for the organisation's management to make the right decisions when controlling and guiding the business continuity management process, it needs information on the current status and development of the business continuity management process. The management must be informed regularly and in an appropriate manner by the contingency planning organisation in management reports regarding the results of the examinations and the status of the business continuity management process. In this report, the problems, successes, and potential improvements must be pointed out.

Management acknowledges receipt of the management reports, evaluates the status, and initiates any corrective measures required. The following aspects must be included in this evaluation:

- Results of the audits (including those of service providers and suppliers)
- Test and exercise results
- Suggested measures after managing a business continuity
- Status of the measures (preventive measures, reactive measures)
- Risks (residual risks, accepted risks, threats and vulnerabilities not taken into account)
- New solutions (products, procedures) for improving the effectiveness (for example tool-based alarming)
- Results of the training and awareness-raising programs
- New standards or best practices (for business continuity management)
- All changes that could have an effect on business continuity management (for example changes to processes outsourced to service providers)
- Implementation status of the measures selected in the last management evaluation

Although the list already contains a variety of different aspects, the management evaluations should be kept short and concise.

The evaluations should lead to improvements in form of corrective measures. These measures can be preventive in nature or also change parts of the business continuity management process. Such changes can include, for example:

- Changes to the budget provided
- Changes to the specified goals and the policy
- Changes in strategies (for individual resources or the overall strategy)
- Changes to the organisational structure of the business continuity organisation
- Changes to processes to react to internal and external requirements
- Changes in the requirements of the business processes
- Changes in the reliability requirements
- Changes in regulatory or contractual requirements
- A change in the level of risk willing to be accepted

It is recommended for the contingency planning organisation to present specific suggestions for measures in the management evaluations submitted to the management to help them make the necessary decisions. The goal of the organisation's management should be to continuously improve the effectiveness of the business continuity management process based on the information in the management evaluations. For this reason, the results of the evaluations and the measures selected for implementation must be documented and the implementation status of these measures checked during the next evaluation. The contingency planning organisation should examine the effectiveness of the newly implemented measures and improve them further, if necessary.

10 Outsourcing and business continuity management

There are a variety of reasons for outsourcing services and business processes ranging from concentration on the most important core competencies and saving costs to shifting risks. Developments have shown that the continuing trend to more and more complex interaction between companies or government agencies and their outsourcing service providers and suppliers lead to a wide variety of contracts, interfaces, and contact persons. However, the advantages from an economic point of view, such as saving costs or concentrating on the core business, come in conjunction with specific risks to the business continuity or security that should not be underestimated. Every outsourcing project is subject to a series of security risks. Additional information on such risks can be found in module 1.11 "Outsourcing" of the IT-Grundschutz Catalogues [GSK].

From the point of view of business continuity management, the outsourcing of business processes means that the number of the risks to the organisation that are beyond the control of the organisation increases. This is naturally associated with a loss of control. In addition, the risks to the internal business processes depending on these service providers also increase. To counteract these risks, various aspects relating to business continuity management must be taken into account when planning and drafting contracts for new outsourcing projects, new delivery agreements, and for outsourcing projects currently underway. Some of these aspects are discussed briefly in the following.

10.1 Planning and drafting contracts

In addition to security management, business continuity management should also be involved in the planning of outsourcing projects. The criticality of the planned service or products to be delivered as well as which new risks arise due to the outsourcing must be examined. The task of the business continuity officer is to ensure that the requirements placed by business continuity management on the business process to be outsourced are taken into account accordingly in the contracts.

If a service is determined to be critical or highly critical, then additional steps should be taken. Depending on the specific criticality level determined, this includes examination of the business continuity management capabilities of the service provider and integration of special clauses or supplements for business continuity management into the contracts.

In addition to the service to be provided, the specific availability requirements of the business processes to be outsourced as determined by the BIA must be analysed and described in detail. Likewise, the business continuity and crisis management capabilities required by the outsourcing service provider must be specified in detail. The service provider must be required to create recovery and restoration plans for the outsourced processes. The operability of these plans must be examined by the business continuity management department of the client. Depending on the outsourced processes and the interfaces between the organisation and the service provider, it may be necessary to hold joint business continuity exercises. The willingness to participate in such exercises as well as the cost allocation for the exercises should be taken into account in the outsourcing contracts. In addition to the joint exercises, the service provider should be able to verify its general business continuity and crisis management capabilities, especially in terms of the outsourced processes, by performing additional, regular tests and exercises. If the service provider expects that the outsourced processes will be impaired when performing internal exercises, then the client must be informed of this well in advance. The level of co-operation expected in an emergency or a crisis must be specified. In addition, the rights and the duties must be specified contractually. Some important rights and duties include to following, for example:

- The outsourcing organisation needs to have the right to obtain information from and conduct tests at the outsourcing service provider so that the internal audit department or an external auditor named by the organisation can perform audits there.
- The duty of the service provider to report must be specified and detailed. For example, the client must be informed of changes to the business continuity management process, to the contingency concepts, or to the contact persons that affect the outsourced processes. Likewise, the client is also required to inform the service provider of any changes that affect the outsourced processes.

- The service provider must report the current status regularly as well as any events, for example the results of audits or any problems relating to business continuity management.
- The contractor should provide data on the service quality continuously (e.g. from the Help Desk) or the client must be granted the corresponding monitoring rights.
- The service provider is required to inform the client of any developments that could impair the proper execution of the outsourced processes.
- It must be specified whether information security or business continuity has higher priority in a crisis so that the service provider can react accordingly.
- Clearly defined escalation levels and paths must be specified by the outsourcing partners so that there are no delays or misunderstandings in an emergency.
- Reaction and availability guarantees must be agreed to by the service provider, including 24 hour per day access to the service provider in case of emergencies.
- The client needs to have the authority to give orders (regarding the outsourced processes) to the service provider when necessary in an emergency or a crisis.
- The outsourcing partners must agree to common rules regarding the possibility and terms of subcontracting the outsourced business processes.
- In the contract, the client should have the right to terminate the contract without notice if the specified requirements are violated or not maintained.

When drafting the contract, the disclaimers, for example for force majeure, should be examined closely to prevent the services to be provided from being excluded from liability in crisis situations.

When selecting a service provider, it should be ensured that it is also possible for the client to use the service provided in an emergency and that compatibility with the contingency planning measures of the client is guaranteed. This includes, for example, the ability of a service provider to provide its services at or to an alternate client site.

10.2 Considerations for the conception

When organising and conceiving the business continuity management system, the outsourced business processes and the supplier must be taken into account in each step. They must be taken into account when performing the business impact analysis and when performing the risk analysis. The goal of the BIA in terms of outsourcing is to identify the requirements in terms of the recovery and restoration of the outsourced processes and compare these requirements to the current contracts to detect any gaps in the service description (e.g. in the maximum downtime, recovery level, or maximum restoration time).

When performing the risk analysis, the interfaces between the outsourced parts and the business processes operated in the organisation and/or the outsourced processes must be examined and the associated risks identified. In this case, both the outsourced processes themselves as well as the interfaces to internal operations represent possible risks. The possible effects of a temporary interruption of an outsourced process must be examined. These effects should be determined for different levels of failure, up to and including total failure of the outsourcing service provider. The corresponding precautions and safeguards must be developed based on this analysis.

The risk analysis should not be limited to the operational phase only, i.e. it should not only examine the current outsourcing contracts, but should also include the migration phase when migrating processes to a new service provider as well as any eventual insourcing phases.

When creating business continuity plans, the interfaces between the internal and outsourced processes must be precisely defined, and the plans must be co-ordinated accordingly. The business continuity procedures of the outsourcing service provider must be compatible with the business continuity procedures of the client. This should be checked during joint tests and exercises conducted by the client and the service provider.

The response to an emergency requires an organisation to co-operate more or less closely with the

service providers, depending on the damage scenario. For this reason, the service description in the contract must also contain rules for escalation, activation of the business continuity response, and activation of the crisis response. The organisation's own business continuity management concept must clearly specify how communication will be conducted to respond to a crisis and how the responsibilities for external crisis communication are distributed.

The outsourced business processes and the external service provider must be included in the regular examination of the business continuity management process and the contingency measures. Verification of the business continuity and crisis management capabilities of the service provider can be provided in the form of a certificate or some other independent examination, but the client must pay close attention to ensure that his outsourced business processes are included in the scope of certification, he is considered one of the key stakeholders, the criticalities of the business processes were set according to the specifications in the contract, and these criticalities are taken into account in the business continuity plans of the service provider.

It is therefore necessary to establish an outsourcing management process that depends on the complexity and criticality of the outsourced business processes. The organisation’s management is responsible for establishing the outsourcing management process. Both sides must name one contact person for this purpose.

11 Tool support

A series of software tools are available for the various tasks and phases of the business continuity management process. The tools available on the market cover different aspects of the business continuity management process. Their features include providing support when determining the business processes, performing and assessing the business impact analysis, performing the risk analysis, creating and updating an business continuity handbook, auditing, conducting tests and exercises, alarming, and providing the reactive business continuity response with support when recording information and evaluating situations, among other features. For example, the following features are available depending on the software used:

- Support for creating and updating business continuity management plans
- Assignment of version numbers, and therefore the ability to assign unique names to the documents relevant to business continuity management
- Control of the update cycle for the documents created using automatic reminder emails
- Creation of an overview of the existing plans for the critical business processes
- Automatic references to individual recovery plans and supported resources (applications and systems) so that each one can be located quickly in an emergency
- Automatic alarming without any delays
- Revision-proof minutes for the crisis team

The use of suitable software tools can make the tasks required to be performed by those involved in the business continuity organisation much easier to perform. Some software products prescribe their own methods and procedural models that the user can use as a starting point for the business impact analysis or risk analysis, for example. The corresponding question and answer schemes are provided and can be implemented and applied immediately without much effort.

When selecting the tool, it should be ensured that it can support an organisation of your type and size. Other criteria for selection can include the following in addition to the general features provided and the cost of the tool, support, and any training necessary:

- The platforms supported or the use of web technologies for platform-independent tools
- Interfaces to other tools already used by the organisation, for example the tools for fault management (help desk), alarming tools, or even inventory or personnel management tools
- User-friendliness, especially for documentation tools
- The ability to create individual views depending on the needs, situation, or role of the user
- Security and data protection for the data stored and administered by the tool (e.g. private telephone numbers, addresses)
- The availability of the tool in a crisis (e.g. access over the Internet)
- The robustness, which is especially important in crisis situations because stressful situations lead to higher error rates

The primary requirements for business continuity management tools from the perspective of information security are as follows:

- The hardware and software must be designed so that the requirements placed on the availability and integrity of the data can be met
- The ability to use secure protocols for communication, e.g. for administration purposes and for remote access, must be provided
- The user administration must be capable of modelling the organisation-wide role concept for business continuity management

- Reliable access control
- The manufacturer must respond promptly to eliminate any security deficiencies detected, provide updates regularly, and release security patches quickly
- Encryption capabilities for especially sensitive data

The following lists some aspects of the security-related selection criteria mentioned above:

- Does the tool support secure protocols for communication? In order to exchange data securely, network enabled tools must support secure protocols, for example SSL/TLS for a browser-based configuration.
- Does the tool have suitable mechanisms for the identification and authentication of the user?
- Does the tool support encrypted storage of passwords or other authentication features used? Tools that store their passwords in unencrypted form should not be purchased any more.
- Is it possible to sign maintenance contracts for the product?
- Can maximum reaction times for eliminating problems be specified in the framework of the maintenance contracts? A maintenance contract is only suitable when the guaranteed reaction and recovery times specified meet the availability requirements of the devices.
- Does the manufacturer offer technical customer service (hotline) that is able to provide help immediately in case of problems? This point should be part of the maintenance contract signed. Pay attention to what languages support is provided on the manufacturer hotline before signing the contract.
- How reliable and fail-proof is the product? The manufacturer should be able to provide reliability data acquired from experience.
- Can the level of detail of the information logged be configured? Does the logging function record all relevant data? Is access to the log data protected? The logging capabilities offered must meet the requirements specified in the security policy at a minimum.

Once all requirements on the product to be purchased have been determined, the products available on the market should be examined to determine the extent to which they fulfil these requirements. Not every product fulfils all requirements at the same time or with the same quality. For this reason, the individual requirements should be weighted based on how important it is to fulfil the corresponding requirement. This evaluation can then be used as the basis for deciding which product to purchase.

12 Glossary

Abbreviations / Terms	Definitions
Alarming	The goal of alarming is to inform the decision-makers responsible and the players as quickly as possible after a damage event occurs so they can initiate the response to the emergency or crisis.
BCM	Business Continuity Management A holistic management process for continuity of the critical business processes in case of an emergency.
BIA	Business Impact Analysis Analysis to determine the potential direct and indirect damage to an organisation caused by an emergency or crisis and the failure of one or more business processes.
CERT	Computer Emergency Response Team Special team of security experts that acts as a co-ordinator to help solve specific security incidents, issues warnings relating to security gaps (also referred to as advisories), and offers approaches to a solution.
Cold site	“Cold sites” are sites that offer all the prerequisites needed to install the necessary equipment, for example IT systems, but at which this equipment has not been installed yet or is not ready for operation yet.
Contingency concept	The contingency concept consists of the contingency planning concept and the business continuity handbook.
Contingency planning concept	The contingency planning concept contains all information required to design the business continuity management process except for the information needed to respond directly to an emergency.
Crisis management	Creation of conceptional, organisational, and technical prerequisites that support the fastest possible return to the normal state after a damage event has occurred. The goal is to ensure the ability of the organisation to make decisions in a crisis and enable a directed and co-ordinated response to the crisis. The organisation-wide crisis management is responsible for all types of crises. Crises in the sense of this standard for business continuity management are a subset of this. Therefore, the response to a crisis in the framework of business continuity management is not the same as full crisis management.
Critical resource	A resource in an organisation whose failure leads to the disruption or failure of a (critical) business process.
Criticality of a business process	Scalable valuation (classification) of the business processes based on their importance to the creation of value in an organisation. The classification is usually based on the recovery requirement for the business process or on the amount of damage to be expected while the business process is down, but additional classification criteria can also be included.

Emergency handbook	The emergency handbook contains all information needed during an emergency or a crisis and for responding to an emergency or a crisis. It therefore contains all business continuity plans such as the crisis communication plan, the crisis team guide, and the recovery and restoration plans
Hot site	“Hot sites” are continuously in operation. When one site fails, a “hot site” can be activated immediately without delay.
KPI	Key Performance Indicator A value used to measure the progress or the degree of fulfilment of a particular objective.
MTPEO	Maximal Tolerable Period of Emergency Operation
MTPD	Maximum Tolerable Period of Disruption Maximal tolerable downtime which, when exceeded, seriously threatens the medium-term or long-term survival of the process or the organisation.
Organisation	The term “organisation” is used as a general term for a government agency, a company, or other types of organisations.
Organisational unit	A logical unit in an organisation. An organisational unit can be a location, a department, a specialised area, or some other unit in the organisational structure, for example.
Restoration time objective	The restoration time objective is the time from the interruption of the process until the start of normal operations. The restoration time objective must be less than or equal to the specified recovery time objective plus the maximum tolerable emergency operation (i.e. < RTO+MTPEO).
RT	Recovery Time Time frame starting with the interruption of a process and ending with the initiation of emergency operation.
RTO	Recovery Time Objective The recovery time of a process or the required resources. The maximum time for recovery must be smaller than the maximum tolerable period of disruption.
Situation centre	Crisis team meeting room The room the crisis team uses to do their work. Special requirements apply to the location and the equipment provided in this room.
Specialised task	A specialised task is the in government agencies used term for a business process.
SLA	Service Level Agreement
Warm site	A “warm site” has a prepared hardware environment including all supply equipment so that this hardware only needs to be configured accordingly or prepared in some other way in an emergency.

Value chain	A value chain is understood to be part of a value-added chain found in the organisation. A value-added chain consists of the entire path of a product or a service from manufacturer to the consumer and therefore can span several organisations.

Other terms and abbreviations used in the document can be found in the glossary of the IT-Grundschutz Catalogues.

Appendix A Strategy options

The following explanations point out the most important options for individual resource classes, but they can only provide a general overview. In all cases, a detailed examination of the environmental variables of the particular company or government agency must be included in the evaluation and selection process. This includes, for example, the risks relevant to the company or government agency in addition to the local service providers.

The following generic strategies can be applied to most of the resource classes:

- Utilisation of internal capacities
- Co-operative partnerships
- Use of commercial capacities and solutions.

A.1 Workplaces

When considering the continuity requirements for workplaces, both the office workplaces needed for the business processes as well as the workplaces in production, including their special equipment requirements, must also be considered. The deciding factor for the selection is the corresponding recovery time objective and the damage scenarios identified.

Distributed business activities

If processes with very short recovery time objectives are operated, then consideration should be given to distributing these processes among several redundant sites. Such redundant sites operate the business function in same manner or in a very similar manner. The necessary resources, including personnel, are always available at such sites. The sites all use the same resources. In an emergency, one of the sites takes over the tasks performed by the site that failed. It is therefore unnecessary to move the personnel to the alternate site. Distribution of the business activities must be prepared in advance so that the tasks can be taken over smoothly. This includes, for example, redundant storage of data or transmission of the data in an emergency. This alternative is ideal for a very short recovery time objective and for bridging the time until alternative workplaces have been set up, but is only partially suitable for use as a long-term solution.

Dedicated internal alternate workplaces

A more expensive alternative is to maintain your own alternate workplaces at an alternate site. This means that there are workplaces available at another location that can be used immediately. Significant investment costs and recurrent costs for maintaining operability can arise depending on the version used (i.e. a warm" or a "hot" site).

Non-dedicated internal solution

If there are rooms available that are not absolutely necessary for maintaining the core business or are only used temporarily, then these rooms can be used temporarily as alternate workplaces. Examples of such rooms include training and meeting rooms or even the cafeteria.

Release

In an emergency, resources from other processes not affected by the emergency and have a lower criticality are used for the critical processes. The processes with lower priorities are operated with fewer resources or even completely shut down. The resources freed can be used temporarily for critical processes.

Telecommuting workplaces and remote access

If the execution of a process is not dependent on its actual location, then employees with the corresponding equipment and access to the Internet can work from any workplace, for example from a

home workplace. Capacity limitations of the Internet connection due to network overloads or at the connection point of the organisation should be monitored and checked, if necessary. There are also other general conditions to take into account in this case. If these workplaces are already being used as home workplaces, then organisational aspects such as the security, software updates, or the use and exchange of the documents required must also be regulated. However, all equipment necessary to perform this work must also be available at the telecommuter workplace. Notebooks used at the workplace in the organisation as well as the telecommuter workplace are only partially suitable since they may be unreachable in the organisation when needed in an emergency and may not be available at the telecommuter workplace.

Co-operative partnership

Partnerships with neighbouring organisations can help overcome crisis situations by accessing the resources of the other organisation, which provides these resources temporarily. Co-operating organisations should have similar organisational structures.

The basic willingness to co-operate in an emergency must be agreed to by the management. The extent to which office space resources of the partner can be used temporarily in an emergency, where these spaces are located, and what computer and performance capacities these rooms are equipped with must be checked in advance. The business continuity co-operation process should be designed in advance and individual assistance options should be gone through together with the affected organisational units to determine their feasibility. The details of this procedure can then be worked out by business continuity management. It is recommended, though, to form a work group containing the persons responsible for business continuity management in each of the co-operating organisations. At the same time, the members of the group can exchange information on current threats and strategies. The risk situation, the market situation, and other general conditions must be re-evaluated regularly and integrated into the agreement. A corresponding duty to perform these re-evaluations should be specified in the agreement and checked regularly to ensure it is up to date.

It is often difficult for neighbouring companies to form such mutual agreements due to the competition existing between them (e.g. when both are providers in the same industry or product field). Counter-espionage measures directed against competitors and similar threat scenarios must be taken into account in all cases.

Commercial solutions from special service providers

A commonly selected variant is to use the services offered by external service providers who are specialised in the preparation of alternate sites or services. Such service providers make the resources specified in advance in the contract available in an emergency so that the business processes can be partially or completely moved to alternate sites in an emergency. The services agreed to in the contract must be specified in detail. Contractual penalties must also be specified in case the services promised in the contract cannot be delivered in the manner agreed to. Since these resources must be reserved at all times in the scope agreed to, this solution results in recurrent costs. These criteria and the availability criteria are the primary factors when making the decision. The availability criteria can consists of criteria relating to the geographic location, the number of different organisations that will use the site in an emergency, and the amount of office space needed, for example.

The following alternatives exist for commercial solutions:

- Permanently assigned alternate site
  A permanent alternate site of an external service provider can be adapted to meet the conditions of the organisation. This alternative has the advantage that a high level of availability is guaranteed, depending on the conditions in the contract. The availability requirements and the other contract conditions can be derived from the results of the BIA and the risk analysis in this case. This variant is expensive, but on the other hand, it guarantees exclusive use of a site that is available without restrictions in an emergency.
- Shared alternate site
  In contrast to a permanent alternate site, a shared alternate site is used by other organisations as well. Depending on the type and effects of the emergency, it is possible for a situation to arise in

which several organisations affected by the emergency want to use the alternate site at the same time. Due to overloads, the alternate site may only be partially available or completely unavailable in such a case. For this reason, the contract agreement must specify if and under what general conditions the selected site is accessible to other customers as well. It is necessary to request information on the other organisations using the site, for example the usage priorities, sizes, and industries of the other organisations. If the service provider cannot clearly state that your organisation will have the necessary space available in an emergency, then shared use of the site with neighbouring organisations should be avoided.

- Mobile alternate site
  Mobile alternate sites include, for example, office containers provided in an emergency or large, specially equipped vehicles. Mobile alternate sites are economical office alternatives for compensating the lost workplaces. However, the space offered by such sites is generally very limited. Suitable set-up sites absolutely must be specified in advance. In addition, it must be examined if the necessary supply lines, e.g. electrical power lines and communication connections, can be guaranteed in an emergency by the service provider or if the client is required to supply these lines.

In an emergency, it may be necessary for employees to work at a remote alternate site. In this case, it must be clarified how to organise the fast and smooth transportation of the employees to this site. If the employees of a company or government agency need to be transferred to the remote alternate site work at the alternate site instead of their usual workplaces for a long time, then the consent of the personnel representative should be requested in advance. Rules must be made relating to the additional time and financial expense resulting from transporting the employees to the site. It may even be necessary to modify the existing work contracts.

A.2 Personnel

Well-trained personnel form the basis for successful implementation of the business processes. Using suitable measures, it must be ensured that that the key personnel are available in emergencies. This includes substitution rules as well as precautions to ensure the necessary personnel can reach the alternate sites in an emergency. Additional information on this can also be found in the Organisation and Personnel modules of the IT-Grundschutz Catalogues [GSK].

It is recommended to create job descriptions containing the necessary qualifications for the key personnel and to create an overview of the employees with their special qualifications to help the business continuity team and aid business continuity capabilities. This includes, for example, experience with the following

- Personal injury (e.g. first aid training)
- Damage to buildings (e.g. experts for fire protection or building services)
- Damage to IT or communication networks (e.g. in-depth IT knowledge).

Substitutes through versatility and cross-training

A program in which the employees are trained in a wide variety of work areas permits flexibility when assigning people to roles in an emergency. The ability to maintain the running processes is therefore distributed among several employees in the organisation. This prevents the organisation from depending on just a few knowledgeable people.

Technical personnel from external providers

Sometimes it is necessary in an emergency to temporarily utilise external technical personnel. It is recommended to create special job requirements or job profiles for the key personnel in advance in co-operation with the corresponding service providers. If necessary, the required provision times should be specified in the contract. If external personnel is only used temporarily, then a corresponding risk analysis must be performed and the appropriate security safeguards implemented.

Knowledge management

A functioning and actively used knowledge management system is necessary to enable the integration of an organisation's own personnel or external personnel into previously unknown processes. It is recommended in this case to provide instructions and solutions to problems that are closely related to practical applications. The information collected should be protected corresponding to its protection requirement, and appropriate security safeguards should be implemented for this purpose. The availability of the data should be ensured through data backup measures.

A.3 Information technology

Most business processes depend on information and communication technology. In this regard, the IT components in particular are especially critical assets. The following explanations provide an overview of possible continuity strategies for information technology, and especially for the operation of computer centres.

Limited IT operation

While performing the BIA, the minimum resources requirements for an emergency as well as the resource priorities for the resources needed for recovery were determined and documented. The business processes are operated at a lower capacity, and therefore operated with fewer resources, in this case.

Redundant IT sites

Special rooms such as server rooms and computer centres are needed to set up the central IT components. There are different types of redundant IT sites depending on the recovery time:

Cold Site
The term "cold site" refers to an alternate site that provides a setup location but that is not equipped with the necessary IT components yet. It meets all requirements for their setup and installation, for example an adequate air conditioning system and electrical power supply, including those requirements resulting from the special properties of the individual IT components. In an emergency, the hardware, software, and data is moved to this site and installed, and the necessary communication connections are established.

Warm Site
A warm site is an alternate site containing a pre-installed hardware environment including all supply equipment. The hardware is set up to the point that it only needs to be activated and the configuration settings specified or changed accordingly in an emergency. The database must be imported, though. Depending on the complexity and the amount of data, putting a warm site into operation can take several hours.

Hot Site
A hot site refers to an alternate site containing a complete and operable infrastructure with a current database. In case the main site fails, a hot site can be activated immediately (possibly even remotely) and can assume the execution of the corresponding tasks with minimal delay. In general, though, it is necessary to relocate the required personnel from the main site to the alternate site.

Information on how to determine a suitable distance between the redundant computer centre and the main site can be found in the BSI publication "Information on the distance between redundant computer centres".

Distributed IT sites

One alternative to a redundant site is to distribute the processes between two or more sites. The alternative site is not only operated in an emergency, rather both sites are operated in parallel as production sites instead. This method further reduces the risks as well as the time lost by activating an alternate site.

A.4 Component failures

When individual components fail, there are various options available to increase the availability and restore operability as quickly as possible, in addition to repairing the components. Examples of components include servers, workplace computers, printers, copiers, and telephones, but also air conditioning systems, emergency power supplies, or parts of a production plant.

Storing components

For especially critical components, a suitable number of backup devices or components in reserve can be maintained. However, there are several points to consider in this case. Additional storage space that is suitable for storing the IT components or other hardware components, for example parts of production plants, is needed. The storage space for the replacement systems should not be located in the same part of the building, and if this is not possible, then at least in a different fire zone. The components stored must match or be compatible with those components used in productive operation, and these components therefore need to be upgraded regularly. Maintaining a reserve of equipment is expensive and prone to error.

Purchasing replacements

If failed components cannot be restored within a tolerable time frame, then replacements should be purchased. To accelerate this process, a current replacement purchasing plan should be available that contains adequate information for each major component in terms of the service description of the components as well as manufacturer and supplier information. If it is possible to list several manufacturers or suppliers for a component, then they should all be listed so that the fastest supplier can be selected in an emergency.

Supplier agreements

Many hardware providers offer special contracts that guarantee the prompt delivery of replacement hardware, even outside of normal business hours. The agreements should contain statements on the specified recovery times. If such a contract is signed, then the geographic distribution of the risks must be taken into account. Neighbouring organisations can be subject to the same crisis scenario in a disaster and may need the same hardware in this case, which means that supply shortages can occur in spite of the contractual agreement. If your availability requirements are high, then additional supply paths should be specified in the contracts, e.g. via ship or air freight. It must also be examined, though, if the supplier is even able to supply replacement hardware from more than just one location.

A.5 Information

Information can be found in companies and government agencies on paper documents, in electronic data, in the minds of the employees, in co-ordinated procedures, or even from the design of the production plants. The information stored digitally and the paper documents are examined when determining the continuity options.

Basic values of information security

Information is especially important, which is why the basic values of classic information security should be taken into account when considering the continuity:

- Confidentiality

  In an emergency, not only the availability, but also the confidentiality of information can be threatened. For example, in the case of a fire, the highest priority is often placed on protecting people and buildings, but not on protecting information. For this reason, it may be necessary to temporarily store confidential information on the street or some other area while rescue attempts are made, which means unauthorised persons could gain access to this information. Likewise, it must be ensured that it is impossible for the external personnel used temporarily in an emergency to gain access to confidential information.

- Integrity

  The integrity of the information can also be threatened by an emergency. A data backup restored after an emergency can contain errors, for example. Databases in particular are especially prone to error when the transaction logs were not completely backed up or not backed up at all and the data resources were then corrupted. However, even the destruction of paper documents (e.g. due to fire or water damage) can lead to missing documentation.

- Availability

  In an emergency, the information on the business processes in the organisation and their restoration processes needs to be available quickly. For this reason, the availability of the business continuity documentation should be ensured using suitable measures, for example by storing copies of the documentation at several different locations.

Data backup, data migration, and archiving

Various requirements need to be placed on the data backup depending on the criticality of the data resources and the availability requirements.

If the resynchronisation points are very short, then various redundant measures (see also module 1.4 Data backup policy in [GSK]) should be used, e.g. mirrors or shadows. They also offer synchronous or asynchronous data transmissions to redundant sites or storage systems. Other options for redundant data storage that can also contribute to fulfilling legal or contractual requirements relating to the archiving of information include:

- Analogue information

  Analogue information such as paper documents or microfilm can be copied and stored at remote storage sites, for example. A suitable method of storing redundant copies of paper documents is to digitalise the documents and store them in electronic archive systems.

- Digital information

  Digital information can be copied to economical storage media and then stored remotely. In this case, it must be ensured that the remote storage location selected is far enough away from the main site, yet close enough to enable the data to be obtained and restored within the specified recovery time objectives. Archive rooms for data backups should meet the same requirements as the rooms in which the data was originally processed.

A.6 External service providers and suppliers

In many organisations, external service providers and suppliers are so integrated into the business processes that these processes cannot be executed as intended when a service provider is temporarily unavailable. This can be due to an emergency, but also due to the service provider declaring bankruptcy or sudden termination of the contract due to inadequate capacity. Possible continuity strategies for this include:

- Transfer of external services to internal services

  If the services supplied by external suppliers can also be provided by internal personnel, then it may be useful to temporarily transfer the services back to your own organisation. To accomplish this, though, the internal personnel must possess the necessary knowledge and be freed from their other tasks. The infrastructure needed by the processes must also be available.

- Redundant and alternative providers

  Services that are especially critical to the continuity of business operations, for example communication connections or the supply of power, can be secured using redundant or alternative providers of the same type. In this case, the geographic independence of the provider and the ability to meet the specified recovery time objectives must also be considered when making this decision.

Appendix B Preventive safeguards

Organisations can take various types of measures for the purpose of prevention. Some of these measures are listed in the following.

B.1 Alarm technology

There are various types of automatic alarm signalling technologies for early detection of a variety of threats. These alarm technologies include, among others, smoke, fire, water, or burglary alarms, for example.

The job of automated alarm technology is to detect any parameters directly or indirectly related to a damage event as early as possible and forward the alarm so that measures to counteract the causes can be initiated promptly. The event detected is then reported to a central location, e.g. a control centre in the organisation or a service provider. Depending on the type of threat, it may also make sense to alarm the immediate environment directly, for example in case of a fire.

When creating the alarm technology concept, the goal should be to increase the probability of detection, enable quick recognition of the relationship between what has been reported and what events triggered the alarms, and, if necessary, to enable a staged reaction procedure for the various areas. The alarm technology should therefore include the following three areas:

- Outside grounds monitoring

  The outside grounds can be monitored using three main types of sensors. This includes the line sensors (for example infrared sensors, hermetic video surveillance), fence alarms, and ground sensors (to the example vibration sensors).

- Interior space monitoring

  The interior space monitoring system secures the area between the outside surface of the building and the actual object to be protected. The requirements for the particular areas to be monitored should documented, and the alarm sensors used must fulfil these requirements.

- Object monitoring

  Individual objects require individual monitoring. For example, the server cabinets need to be monitored individually for temperature changes, and the performance of IT components need to be monitored individually.

Alarm systems are specially categorised according to the particular monitoring task in terms of where they can be used, their function, and their requirements. The following points should be taken into account for this reason before configuring an alarm system:

- Environmental parameters
- Power supply required
- Possible sources of interference
- Insurmountability
- User-friendliness and ease of maintenance

An alarm system consists of a number of local sensors that communicate with a central alarm unit, which then triggers an alarm when necessary. If a burglary, fire, water, or gas alarm system is already installed, then the core areas of the organisation at a minimum should be monitored with these systems so that threats can be detected early and countermeasures initiated. The alarms must be forwarded to a location where someone is on duty at all times (i.e. to the gatekeeper, security guards, security service, fire department, etc.). In this case, it must be ensured that this location is also able to react appropriately to the alarm in terms of technology and personnel.

An alarm system is a complex overall system that, on the one hand, is adapted to the building as well

as to the individual business processes and, on the other hand, needs to be planned and installed by the corresponding organisation while taking the expected risks into account.

Alarms should be transmitted to a central control centre. A control and communication system must be integrated into the organisation to provide support for this control centre. Depending on the monitoring sensors installed and other external parameters, the employees in the control centre of an organisation should have access to the following technical documents and equipment:

- Location plan showing the positions of all sensors
- Monitors for video surveillance
- Computers with large displays for logging purposes to guarantee a lower error rate when reading information in stressful situations
- Telephone and fax connections
- Possibly a telephone system with a direct line to security forces (fire department, police)
- Radio base station with direct connections to the mobile communication devices used by the security forces (reserve radio devices for additional security forces in an emergency)
- Archive for plans, drawings, and object-specific documents (property plans)

To plan future measures and measure their effectiveness, detailed documentation of all security incidents and alarms sent within the alarm system is necessary. This information can be acquired manually by people (by taking tours or similar inspections) as well as by information systems. The information to be documented includes:

- Current status reports from people or sensors
- Damage reports and damage management
- Reported alarms
- Reaction measures taken
- Object-based and function-based auxiliary information (for example plans and checklists)

In addition, historical reference data from past damaging events should be documented in order to gain knowledge from comparable incidents.

B.2 Data backup

Information represents an important asset to every organisation, regardless of whether this information is available in analogue or digital form. If material resources are destroyed or become unusable, then they can be restored by purchasing them from suppliers, external service providers, or through other means in most cases. In contrast, the information stored on data media is always lost for good if the data media are destroyed or damaged. For this reason, it is necessary to implement special measures to back up the data.

As described in module 1.4 Data backup policy in the IT-Grundschutz Catalogues [GSK], it is necessary to create corresponding data backup policies in an organisation.

B.3 Agreements with external service providers

If a continuity strategy was specified in which the support of commercial providers of business continuity services are utilised to respond to an emergency, then criteria similar to those for outsourcing should be used when selecting the provider and the type of contract. The most important points in this regard are described in the IT-Grundschutz Catalogues [GSK] in module 1.11 Outsourcing.

There are a number of services offered to prepare for an emergency. These services include, for example, the operation of an alternate computer centre, alternate applications, or alternate IT components, but can also include alternate workplaces or the provision of trained personnel for certain

areas. If the organisation has decided to use external business continuity services, then the main requirements for the services provided must be specified. These requirements form the basis for the selection of a suitable provider.

For this reason, it is important to work out suitable test points during the process of selecting the provider. Based on these test points, contracts should be signed with those service providers meeting all these criteria.

In this case, offers should be obtained from a variety of different providers. To do this, the cornerstones of the planned contract should be sketched out in a requirements profile, and then a requirements specification should be created based on this profile. This requirements specification forms the basis later on for the assessment and selection of the services offered. All future contractual agreements should also be based on the requirements specification. It is therefore necessary to provide detailed information on the expected services. To guarantee that the services agreed to completely cover all critical business processes, all relevant organisational units and roles must be involved in the development of the requirements specification. These organisational units and roles can include, for example:

- Building management
- Persons responsible for the contingency planning
- Employees in information technology
- Purchasing and procurement department
- Legal department

It is recommended to create catalogues of questions listing the requirements for a service provider. In this case, the following points should be included, for example:

- Areas of experience, size, and location of the provider
- References from the provider
- Verification of quality or certification, e.g. according to ISO 27001 based on IT-Grundschutz
- Service and support provided for the business continuity management/response process
- Test and exercise capabilities
- Initial costs, annual costs, costs when services are used, costs for participation in tests and exercises
- Ability of the provider to adapt to the needs of the client
- Resource-related requirements (guaranteed time frames, reaction times, etc.)
- Communication interfaces
- Well-founded security and contingency planning concept of the provider
- Ability to examine internal audits

The requirements profile depends greatly on the types of business continuity services that will be used. For this reason, the evaluation criteria must be adapted to the special conditions, and each criterion must be weighted accordingly.

Once the decision has been made to use a certain provider, all criteria relevant to business continuity management should be secured contractually.

This contract must also clarify the exact conditions of the co-operation, e.g. it must state the contact persons, substitutes, reaction times, IT connections, performance controls, design of the IT security precautions, handling of confidential information, copyrights, documentation duties, rules relating to the disclosure of information to third parties.

B.4 Specification of alternate sites and their requirements

During the planning performed in the framework of contingency planning, one or more alternate sites, both for the office or production building as well as for IT operations, must be selected for some scenarios.

A minimum of the following points must be taken into account when creating the contingency planning concept:

- How to reach the alternate site (transportation methods and routes), and if necessary, how to transport the employees to the alternate site
- Requirements placed on the site (space requirement, infrastructure, and security safeguards such as access protection)
- Lines of communication and communication medium (How many telephone cards will be needed? Who will switch over the telephones and fax machines? How many telephone and fax connections and devices must be available at a minimum?)
- Network connection to the site (e.g. WAN connection to the organisation's computer centre or IT connection over the Internet). In this case, the bandwidth, IP addresses, and security safeguards such as the type and configuration of the firewall system, etc., must be clarified, among other things.
- Ability to reach the employees and their representatives at the alternate site and/or at home (telephone number, cell phone number, email address)
- Measures and responsibilities for putting the alternate site into operation so that the alternate site is up and functioning and the employees can move in within the required time
- Measures and responsibilities for taking the alternate site out of operation after responding to an emergency, i.e. who is responsible for this and how the alternate site will be returned to the same state as before the emergency. This includes, for example, switching back the telephone lines or redirecting IP addresses.

Appendix C Outline for the business continuity handbook

A business continuity handbook must be designed so that another expert is able to perform the business continuity measures specified in the manual. The following presents a sample Table of Contents for a business continuity handbook for use as a basic guide. The sections of the suggested outline your organisation uses depends on which system and application documentation is available and must be selected on a case-by-base basis.

Note: The proper organisation and layout for a business continuity handbook for an organisation depends on the size and structure of the organisation. This example only serves as a suggestion and must be adapted to the particular conditions of the organisation.

1. Introduction
   - 1.1. General information: Name of the organisation, scope, etc.
   - 1.2. Document control: Version, distributor, specification of the person responsible for the document, classification of the document, etc.
   - 1.3. Index of abbreviations
   - …
2. Immediate measures
   - 2.1. Specific tasks for individual persons/roles in an emergency
   - 2.2. Instructions for special emergencies
   - …
3. Crisis management
   - 3.1. Roles, responsibilities, and authorities
   - 3.2. Reporting paths and escalation
   - 3.3. Crisis team meeting room / Situation Centre
     - 3.3.1. Sites, accessibility, ...
     - 3.3.2. Preparation of the emergency meeting point
   - 3.4. Working on the crisis team
   - 3.5. Assessment of the situation
   - 3.6. Documentation in the crisis team
   - 3.7. De-escalation
   - 3.8. Analysis and assessment of the business continuity response
4. Communication and public relations in a crisis
   - …
5. Restoration
   - 5.1. Restoration of the office spaces
   - 5.2. Restoration of the infrastructure
   - 5.3. Restoration of the IT
   - 5.4. Restoration of the communication connections
   - …
6. Business continuity
   - 6.1. Availability requirements of the organisational units

6.2. Business continuity plans

6.2.1. Organisational units with criticality A

6.2.2. Organisational units with criticality B

6.2.3. Organisational units with criticality C

…

6.3. Analysis of the recovery and restoration

…

7. Appendix

7.1. Accessibility of the members of the business continuity team

7.2. Emergency numbers (e.g. fire department, police, emergency doctor, water and electrical power providers, alternate computer centre, external data media archives, external telecommunication providers)

7.3. Additional/supporting plans and lists

Appendix D Outline of a business continuity plan

The following presents an example of a possible Table of Contents for a business continuity plan. Which sections of the suggested outline your organisation can use depends on the structure of the organisation and the business processes and must be selected on a case-by-case basis.

1. Introduction
   - General information: Name of the organisation, name of the plan, goals of the plan, scope, etc.
   - Activation and deactivation of the plan
   - Document control: Version, distributor, specification of the person responsible for the documents, classification of the document, etc.
   - Index of abbreviations
   - Relevant and associated documents
2. Business continuity crew for the organisational unit
   - Person responsible
   - Business continuity team, duties, and authorities
   - Alarming and escalation
3. Recovery of the business processes
   - Recovery strategy
   - Recovery goals and maximum duration of emergency operation
   - Resource requirements of the processes
   - Alternatives for emergency and alternate operation
   - Returning to normal operation
   - Post-emergency tasks
4. Scenarios
   - Single-site failure" scenario
     - Requirements for the alternate site
     - Resources needed at the alternate site
     - Reactive measures for recovery
     - Changes to workflows during emergency operation
     - Measures for restoration and returning to normal operation
     - …
   - "Information technology failure" scenario
     - Follow-up scenarios
     - Requirements placed on emergency operation
     - "Examination of the particular application / of the particular system"
     - Replacement purchasing plan

     ...

- "Loss of personnel" scenario
  - Follow-up scenarios
  - Requirements placed on emergency operation
  - Reactive safeguards for the recovery
  - Changes to workflows during emergency operation
  - Measures for restoration and returning to normal operation
- "Service provider failure" scenario
  - Follow-up scenarios
  - Reactive measures for recovery
  - Changes to process flows during emergency operation
  - Measures for restoration and returning to normal operation
  - …

5. Additional information
   - Sites
   - Directions for getting to the sites
   - …
6. Contact information
   - Lists of employees
   - Service providers
   - …
7. Appendix
   - Forms, templates, checklists

Reference documents

Words of thanks

The Federal Office for Information Security was provided with the support of experts in the field to develop this guide. We would like to thank everyone who made this standard possible and accompanied it through its development.

BSI Standard 100-4 is based on a draft created by HiSolutions AG, who was contracted by the BSI for this purpose. We would like to thank the authors, Robert Kallwies, Timo Kob, Stefan Nees, and Björn Schmelter, who helped make this standard possible.

We would also like to thank the following experts and organisations who, through their contributions, quality control support, and helpful discussions, gave the standard a significant push forward. They deserve special thanks since their motivation was what made the creation and refinement of this BSI standard possible in the first place.

- Thomas Bittl, Federal Office for Mail and Telecommunication
- consequa GmbH
- Ulrich Dreyer, 3R-Kontext
- Ingo Geisler, Vodafone D2 GmbH
- Matthias Hämmerle, KPMG AG
- Dr. Armin Hampel, Hewlett-Packard GmbH
- Dr. Wolfgang Mahr, Axept AG
- Michael Müller, KPMG AG
- Uwe Naujoks, UKN Management Consulting
- Markus Riedl, Bavarian Ministry of the Interior
- Thomas Teichmann, Schmitz & Teichmann Betriebsberatung GmbH
- Astrid Wiesendorf, Vodafone D2 GmbH

The following employees of the BSI participated in the creation of BSI Standard 100-4: Dr. Marie-Luise Moschgath, Isabel Münch, Dr. Harald Niggemann.