Business Continuity Management for SMEs using the Cloud

Higher reliability of IT-supported business processes in SMEs using cloud services
Acknowledgements

The BSI would like to thank Mr Christoph Puppe and Mr Alexander Papitsch from HiSolutions AG for their contributions to the preparation of this study. The BSI would also like to thank Mr Alexander Reichenberger from ACP Solutions for the helpful comments and discussions.
# Table of Contents

Acknowledgements ............................................................................................................................................ 3

1 Introduction .................................................................................................................................................. 7
  1.1 State of Affairs: BCM in SMEs ........................................................................................................... 7
  1.2 Definition of the term “cloud” .............................................................................................................. 8
  1.3 Applicability .......................................................................................................................................... 8
  1.4 Scope .................................................................................................................................................. 9

2 Selected Aspects of Business Continuity Management ............................................................................. 10
  2.1 Overview ........................................................................................................................................... 10
  2.2 Business Continuity Management Goals ............................................................................................ 11
  2.3 Contingency Prevention ...................................................................................................................... 11
  2.4 Differences between Malfunction, Contingency and Crisis ................................................................. 12
  2.5 Business Continuity Management Process .......................................................................................... 13
  2.7 Business Impact Analyses .................................................................................................................. 15
    2.7.1 Business Processes and Resources ................................................................................................. 15
    2.7.2 Damage scenarios ......................................................................................................................... 16
    2.7.3 Classes of Effect ............................................................................................................................ 16
    2.7.4 Time Horizons .............................................................................................................................. 18
    2.7.5 Determining the Maximum Tolerable Period of Disruption (MTPD) ............................................. 18
    2.7.6 Form to carry out an IT BIA ........................................................................................................... 19

3 Business Continuity Management in Private Cloud usecases ..................................................................... 20
  3.1 Private Cloud and Virtualisation ......................................................................................................... 20
  3.2 Contingency Prevention ...................................................................................................................... 20
  3.3 Multiple Sites ..................................................................................................................................... 21
    3.3.1 Replication and Amounts of Data ................................................................................................. 21
  3.4 Particularities of the Business Continuity Management Process ......................................................... 22
  3.5 Tests and Exercises ............................................................................................................................. 22

4 Business Continuity Management using the Hybrid and Public Clouds .................................................... 24
  4.1 Software as a Service (Saas) and Platform as a Service (PaaS) ............................................................ 24
  4.2 Disaster Recovery as a Service (DRaaS) .............................................................................................. 25
  4.3 Virtual Site at the Provider ................................................................................................................... 25
  4.4 Remote Backup / Backup as a Service ................................................................................................. 26
    4.4.1 Data Backup on the Client ............................................................................................................ 27
  4.5 Data Backup using IaaS and SaaS ....................................................................................................... 28
  4.6 Technical Personnel with Cloud Authorities ....................................................................................... 28
  4.7 Internet Connection of the Business Premises ................................................................................. 28
  4.8 Mobile Connection to the Public Cloud .............................................................................................. 29
  4.9 Authentication .................................................................................................................................... 29
    4.9.1 Two-Factor Authentication ........................................................................................................... 30
  4.10 Selection of the Cloud Provider ......................................................................................................... 30
    4.10.1 Taking the criticality into Account ............................................................................................. 31
    4.10.2 Interface to Business Continuity Management ......................................................................... 31
Table of Contents

4.10.3 Provider Availability ................................................................. 31
4.10.4 Medium-sized Partners for the SMEs ......................................... 32
5 Contingency Planning when using the Public Cloud ......................... 33
6 Data Protection and Cloud .............................................................. 36
7 Scenarios for Contingency Planning in SMEs ................................... 37
  7.1 Scenario 1: All Applications in the Public Cloud ......................... 37
  7.2 Scenario 2: Private Cloud and Backup in the Public Cloud ........... 38
  7.3 Scenario 3: Additional Site in the Cloud ..................................... 39
8 Conclusion and Outlook .................................................................. 41
9 Appendix: Example of an IT-BIA of a SME .................................... 42
  9.1 Financial Accounting ................................................................. 42
  9.2 Distribution ................................................................................ 43
  9.3 Production .................................................................................. 44
  9.4 IT Systems and Providers requiring Special Protection .................. 45

References ......................................................................................... 46

List of Figures
Figure 1: Phases of the Business Continuity Management Process .................. 14

List of Tables
Table 1: Malfunctions, emergencies, crises and disasters as understood in BSI Standard 100-4 ......................... 13
Table 2: Example criteria of the classes of effect ........................................ 18
Table 3: Form to carry out the IT BIA .................................................... 19
Table 4: Experiences with replications of the cloud service provider ACP Solutions (by courtesy of Thomas Reichenberger from ACP Solutions) ......................................................... 22
Table 5: Failure scenarios of the business continuity management and corresponding reactions for a SME. 35
1 Introduction

Due to a relatively tight budget which SMEs are able to invest in information security, it is not surprising that in many SMEs no comprehensive business continuity management process is established. This fact has also been confirmed by the study conducted by the BSI on the IT security in small and medium-sized enterprises [BSI_2011a]: According to this study, "less than half of the companies have implemented any business continuity management. However, this is not caused by ignorance, but rather by cost savings and the inadequate assessment of the risk to be borne."

This study on the subject of "Business Continuity Management for SMEs using the Cloud" examines the potentials of cloud technologies for the protection of IT-supported business processes in SMEs which can be foreseen today. The objective is to present practical contingency prevention and contingency response methods using modern technologies. Thus, a consideration of the use of the cloud offerings for business continuity management of SMEs available on the market and a consideration of their application in three typical scenarios is focussed in this document. These scenarios are intended to illustrate how the application of cloud technologies can improve the business continuity management and various continuity strategies for the better.

At the moment, the use of cloud and virtualisation technologies is mainly promoted in terms of reducing costs. This study is to make clear that a higher level of availability and reliability of business processes can also be achieved almost automatically using cloud and virtualisation technologies. This additional potential, which has so far been paid too little attention and is particularly interesting for SMEs with limited resources for business continuity management, is examined in this document.

On the basis of real world examples from practice, it is illustrated how virtualisation has already been used in some SMEs to keep the potentially disastrous effects of contingencies (failure of information technology due to fire or water, for instance) as low as possible.

As an introduction to business continuity management, this document first provides a rough outline of business continuity management according to the BSI Standard 100-4. This should point out to the reader which questions a person in charge has to address when introducing a comprehensive business continuity management.

1.1 State of Affairs: BCM in SMEs

Business continuity management is a very under-represented subject in the IT of SMEs. So far only few publications and practical guides supporting SMEs in establishing an adequate business continuity management are available. Standard 100-4 published by the BSI for business continuity management is comprehensive, but is often considered to be too complex for this company size. This group of companies, which is very important for Germany’s economy, usually has neither the personnel nor the financial resources to implement comprehensive business continuity management in their own companies.

At the same, many SMEs use virtualisation technologies, build up their own private cloud capacities or use public cloud offerings. According to a study conducted by Dell and Intel in 2012 [DI_2012], at least approx. 41 percent of the SMEs have already applied virtualisation; however, only approx. 17 percent of all SMEs interviewed use the cloud computing options. However, the potentials associated with the application of virtualisation and cloud technologies to protect business processes against failure are rarely used.

Previous approaches to protect IT-supported business processes against failure include having corresponding hardware available twice or to quickly purchase new hardware after an contingency. Both solutions are costly and time-consuming. A majority of the smaller SMEs have a very sceptical opinion regarding the use of a redundant arrangement of components and would rather accept a longer failure of a system than purchase an additional server which would then be located in the same computer centre with the same power supply anyway. If there is a power failure, both servers would be affected. In order to be really able to operate systems redundantly, a redundant power supply as well as an uninterruptible power
supply (UPS) or the installation of the components in geographically distributed computer centres would also have to be taken into consideration, which, in most cases, is not feasible for smaller SMEs in particular for cost reasons.

Using application of virtualisation and cloud technologies, the contingency planning costs and the time required for recovery can be reduced significantly. Thus, cloud technologies are a driver for innovation in business continuity management. Especially for small and medium-sized enterprises, corresponding offerings are interesting, as SMEs can build up double capacities such as a second site for data processing and data storage redundancies thanks to these offerings.

1.2 Definition of the term "cloud"

Cloud computing is understood by the BSI as offering, using and billing IT services dynamically adapted to the requirements via a network. Here, these services are only offered and used by means of defined technical interfaces and logs. The range of the services offered within the cloud computing framework covers the entire spectrum of information technology and, among other things, includes infrastructure (e.g. computing power, storage space), platforms and software.

In this respect, the services can either be obtained from a public, private or hybrid cloud. In a public cloud, the offered services can be used by any person. A private cloud is referred to if the company operates both the services and the infrastructure itself. If services of a public cloud are used from a private cloud or if several cloud infrastructures, each of which are autonomously themselves, are used jointly using a standardised interfaces, this is referred to as a hybrid cloud.

As this is based on using virtualisation technologies in most cases, an application of a virtualised environment is often also referred to as a private cloud. In this study, the two terms are used synonymously.

According to recent surveys, the global demand for cloud services will increase substantially in the next few years. There are multiple reasons for the rising interest in cloud computing and the increasing use of cloud services. Cloud computing promises a very high level of flexibility when booking and using as well as withdrawing from computer centre capacities depending on the current requirements. A high saving potential regarding the IT systems which must otherwise be made available, maintained and replaced locally is also expected. Another advantage of cloud computing is the ubiquitous availability of business applications, which is particularly elaborated on in this document.

When using the public cloud, companies are enabled to act flexibly in order to respond quickly to changes in the market. For example, new services can be provided more quickly and without having to purchase expensive hardware; capacities can be adapted dynamically to the demand and thus adjust better to changed requirements than rigid IT infrastructures. There are no costs for the purchasing, operation and maintenance of hardware. Instead, almost unlimited resources are available without IT technical personnel having to deal with the installation, configuration and maintenance of hard- and software.

The BSI has published an Eckpunktepapier [BSI_2012a] on how to use public clouds. If public cloud computing is used for the company’s own business continuity management, all aspects mentioned there must be examined and compared regarding compatibility with its own requirements, for example with requirements resulting from the BIA. In general, using public cloud offerings is less expensive than operating one’s own infrastructure. Still, the amount of planning is higher or has a changed focus and additional contractual and data protection aspects to be outlined in this document must be considered.

1.3 Applicability

This study and the scenarios presented therein can be applied to companies employing between 10 and 500 employees. The study also assumes normal protection requirements of the data and business processes.
1.4 Scope

A company placing special requirements on the availability of business processes and data can orientate itself on this study, but is encouraged to clarify for itself when defining the protection requirements which goals it should reasonably specify in information security management and business continuity management.

Another restriction and differentiation is the focus regarding the resources examined. The study focusses on the protection of the IT resources and the required IT service providers. The resource classes of personnel, buildings and non-IT infrastructure are not explicitly examined in this study, as cloud and/or virtualisation technologies cannot protect these resource classes directly.
2 Selected Aspects of Business Continuity Management

Business Continuity Management is a systematic approach oriented towards the business processes of an organisation as a precaution against and response to contingencies (and in some cases also crises). It is intended to restrict at least the damaging effects of such exceptional situations if they cannot be prevented entirely. This includes building up organisational structures as well as developing and implementing concepts allowing a quick response to contingencies and the continuation of at least the most important business processes. In this respect, the term "business process" does not only refer to the economical and productive processes of companies, but in general all processes of a company or a government agency with which it renders its services and fulfils the respective technical tasks.

2.1 Overview

An introduction to the subject of “Business Continuity Management” is provided by the Business Continuity Management webinar [BSI_2012b], explaining BSI Standard 100-4 and giving an understanding of the practical implementation using several application examples. Several contents of this chapter are taken from this webinar or the standard itself.

Standard 100-4 published by the BSI describes a methodology for establishing a business continuity management system based on and extending upon the the procedure for implementing a management system for information security described in BSI Standard 100-2 [BSI_2008].

The goal of Standard 100-4 is to present suitable solutions to quickly respond to contingencies and crises of different origins that might result in interruptions of business operations. In general, larger organisations have separate business continuity and crisis management systems and strictly differentiate between contingencies and crises. SMEs – the addressees of this document – do not have these resources, which is why both cases are to be addressed by means of business continuity management. In addition, the Standard describes preventive methods and procedures to prevent contingencies and crises or to at least reduce their effects.

The business continuity management should examine damage events of the categories

- Malfunction
- Contingency and
- Crisis (in part)

in order to be able to respond to it adequately. This means to ensure that malfunctions do not result in contingencies and that contingencies do not escalate into crises and to support crisis management on the operational side in the event of a crisis. A central role in the business continuity management according to the BSI Standard 100-4 is fulfilled by the BCM manager who manages all activities concerning the contingency planning and is involved in the associated activities. In general, a SME does not employ a person who only fulfils the role of the BCM manager, but the role of the BCM manager is assumed, for example, by the the Head of IT or the IT Security Officer. As this study covers only the protection of IT-supported business processes anyway, this situation, however, in which an employee assumes a role and is still responsible for doing his normal job is not critical. Only if an organisation also wants to protect business processes which are not supported by means of IT within the business continuity management framework, should such a double-role situation be examined critically.

The starting point of any business continuity concept is the Business Impact Analysis (BIA). In this analysis, business processes are identified, prioritised according to their criticality, connected to process chains, required resources of the business processes are identified and the operational levels are defined for...
Selected Aspects of Business Continuity Management

contingency operation. Business processes and resources identified as critical are particularly protected within the business continuity management framework.

The BIA procedure described in the BSI standard is complex and is rarely applied fully in SMEs. Experience has shown, however, that the business processes to be protected are the same in many SMEs. Thus, it is not at all necessary for each SME to start from scratch, but it can start with the standardised business processes, criticalities and resources referred to in this study and modify them according to its own considerations. This approach is considerably more resource-saving and efficient and represents the core of the BIA process presented in this study.

The primary goal of business continuity management is to ensure the continuity of business processes during or after an contingency. Thus, specific continuity strategies to be applied to critical business processes must be developed. In this respect, factors such as the recovery time following an contingency, the implementation costs as well as the reliability of the solution play a vital role.

Therefore, a comprehensive business continuity management consists of the following parts:

• Initiation of the business continuity management process
• Conception
• Business Impact Analysis (BIA)
• Risk Analysis (RA)
• Continuity strategies
• Contingency planning concept
• Contingency response and crisis management
• Tests and exercises
• Maintenance and continuous improvement

When preparing a solution to protect the continuity of a business process, it is primarily a question of the costs and the risk appetite if a prepared continuity solution is to be actually implemented.

In addition to these simplifications of the business continuity management in SMEs, virtualised environments in all organisations have an influence on both the business continuity management process as a whole and the contents of the business continuity management itself. This is to be explained in the following subsections.

2.2 Business Continuity Management Goals

The main goal of the business continuity management is always to prepare the company well for the contingency (prevention) and to reduce the consequences of an contingency to an acceptable level (response). The core of the business continuity management is to protect the company against closing down the business due to excessive losses caused by an contingency.

2.3 Contingency Prevention

The term "contingency prevention" covers all safeguards either preventing the damage event from occurring or ensuring that the damage is kept to minimum if the damage event occurs.

A simple example for such prevention is a synchronously mirrored server farm with double redundancies which is installed in two different parts of the building. If one of the rooms is destroyed by penetrating water, all applications can still be run and the users can continue to work in an unimpeded manner. In the
past, only large companies were able to build up and operate such redundancies; today, this is also possible in a SME thanks to virtualisation and cloud technologies.

2.4 Differences between Malfunction, Contingency and Crisis

Minor malfunctions occur time and again in all organisations. Short-term power failures, shortages in personnel, services are rendered with delay or devices become defective. For such incidents, there are usually simple solutions available which are an integral part of the daily routine. For example, power generators are activated, overtime worked, production times prolonged or replacement devices purchased. In addition, the possible damage of such events is minor from the point of view of the affected organisation.

Only if malfunctions or failures cause major damage and their elimination is no longer possible applying the usual procedures, they are considered as an contingency and require business continuity management.

The following examples are possible contingencies:

- Due to fire, important business premises (e.g. the server room) can no longer be used.
- Flooding results in access roads being blocked for several days.
- Germs in the food in the canteen cause a significant shortage of personnel.
- The power supply system fails extensively and over a longer period of time.
- Important communication networks (Internet, telephone network) fail for several days.
- Important services fail completely because an external organisation was forced to file for bankruptcy and it is also not possible to contract another service provider as substitute.

All these events can also escalate into crises or disasters. Crises differ from contingencies in that concrete plans can be prepared to respond to contingencies, whereas crises cannot be foreseen in most cases and, thus, cannot be handled using concrete precautions and plans. Although this is the most obvious difference between crisis and business continuity management, the two management systems are closely connected: A business continuity management is a good preliminary stage for the crisis management of an organisation and the more comprehensive the business continuity management is, the less likely the escalation into a crisis for the organisation is. In addition, the concrete plans of the business continuity teams can support the operative work of the crisis management. For this reason, business continuity management was formerly referred to as "operative crisis management".

The following table briefly explains the differences between malfunctions, emergencies, crises and disasters according to BSI Standard 100-4 and summarises when and in which way the business continuity management is responsible for handling them.
<table>
<thead>
<tr>
<th>Type of incident</th>
<th>Explanation</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malfunction</td>
<td>Short-term failure of processes or resources with only low damage</td>
<td>Response is part of the usual troubleshooting.</td>
</tr>
<tr>
<td>Contingency</td>
<td>Long-term failure of critical processes or resources with a high or very high level of damage</td>
<td>Response requires special business continuity organisation.</td>
</tr>
<tr>
<td>Crisis</td>
<td>Aggravated contingency primarily limited to the organisation which puts the existence of the organisation at risk or affects the health or life of persons.</td>
<td>As crises do not affect the environment or public life extensively, they can, at least for the most part, be resolved within the organisation itself.</td>
</tr>
<tr>
<td>Disaster</td>
<td>Large-scale damage event which is not limited spatially and temporally, with effects on the environment and public life. For example, as a result of a leakage of a chemical tank.</td>
<td>From the organisation's point of view, a disaster is considered to be a crisis and is handled internally by its contingency and crisis team in co-operation with the external aid organisations.</td>
</tr>
</tbody>
</table>

Table 1: Malfunctions, emergencies, crises and disasters as understood in BSI Standard 100-4

2.5 Business Continuity Management Process

The preventive tasks in business continuity management are described on the basis of a process model aimed at continuous improvement.

For this purpose, the BSI Standard 100-4 distinguishes between the following six phases:

- **Initiation**
  Supported by the management of the government agency or company, strategic objectives are established and the essential organisational framework is set up for the business continuity management process in an organisation.

- **Conception**
  The critical business processes and resources of an organisation are determined and the risks to which it is exposed is evaluated. Consistent with these evaluations, preventive and reactive business continuity strategies and safeguards are developed.

- **Implementation of the contingency planning concept**
  The priorities for the implementation of the contingency planning concepts are specified, resources are made available, responsibilities are defined and, if necessary, required accompanying safeguards identified.

- **Contingency response**
  The responsibilities, plans and codes of conduct for responding to and acting in contingencies are laid down in a business continuity handbook.

- **Tests and exercises**
  Contingency precautions and business continuity plans are tested and practised to check the operability, identify possible defects and to train behaviour in the event of an contingency.

- **Maintenance and continuous improvement**
  The appropriateness and effectiveness of the concepts and safeguards are checked at regular intervals.
Together with an analysis of the results of the tests and exercises, these checks contribute to the continuous improvement of the business continuity management process.

The business continuity management process according to BSI Standard 100-4 is also shown graphically in the figure below.

![Figure 1: Phases of the Business Continuity Management Process](image)

### 2.6 Particularities of the Business Continuity Management Process in Virtualised Environments

Virtualisation has led to rethinking in all areas of IT operations. This statement also holds true for business continuity management. The standardisation of the virtual hardware in particular solves many problems. Thus, it is no longer necessary to purchase identical hardware in order to be able to re-install system backups. Another contribution to the simplification is the fact that it is very easy to operate any servers in a cluster established by virtualisation. Thus, it is now also possible for services not designed for high availability to move very quickly production into the second cluster in another room. Thanks to
virtualisation, availability classes are now available to SMEs which were only reserved to larger companies a few years ago.

In addition to technical contingency planning, contingency planning with the processes for recovery is also affected by the rethinking regarding virtualisation. Thus, the focus changes from recovery and its planning to a mere control of switching successfully to the clusters. Today, planning for contingency operation is rather resource planning within the virtualised environment instead of site planning. This applies at least to the servers. Business continuity management for clients is also affected by the upheaval, as the central terminal server becomes more important with the increased use of server-based computing and the thin clients used for this purpose and also benefits from the advantages of virtualisation.

With the introduction of virtualisation and cloud technologies, the aspect of integrity of information security has gained particular importance. Whereas, without virtualisation, violated integrity can result in individual files no longer being readable, an unreadable image file in virtualised environments means that the servers or clients contained in these no longer function. The integrity of the data and, thus, the protection of the consistency of the replications of images and other files in particular is therefore of much greater importance in virtualised environments and must be paid particular attention in the planning and implementation phase.

2.7 Business Impact Analyses

For contingency planning, the purpose of the business impact analysis (BIA) is to identify those business processes and resources supporting these processes which are particularly critical for the company and, thus, must be given special protection against failures and loss of data.

On the basis of a damage event which is not described in greater detail, it is determined in a BIA how high the damage for the company would be if business processes are interrupted by an event. A complete BIA examines the failure scenarios of failure of buildings, infrastructure (this includes the IT), personnel and service providers. In this document, we are only concentrating on the IT, as contingency planning using cloud technologies can only directly protect the IT. Thus, it would be possible in this case to talk of an IT BIA. However, the IT BIA is designed in such a manner that it can be integrated seamlessly into a general BIA.

Since the procedure of a BIA described in BSI Standard 100-4 is very complex and comprehensive, this study recommends a procedure adapted to the requirements of a SME in order to determine the critical resources on the basis of business processes occurring in all companies.

2.7.1 Business Processes and Resources

In the first step, the business processes to be considered must be defined. In order to simplify the BIA, typical core processes of SMEs are presented below. In addition, it is determined which effects a failure of IT components or IT service providers would have.

Experience has shown that the processes listed here are given the highest priority in SMEs and should thus be protected within the business continuity management framework. The users of the study on the subject of "cloud and business continuity management" only have to compare this prioritisation to their own requirements. Likewise, these processes in SMEs often require comparable resources, i.e. IT systems and IT service providers. The core processes under review include:

- Financial accounting including
  - payroll accounting
  - Invoicing
  - Taxes, especially turnover taxes
2 Selected Aspects of Business Continuity Management

- Distribution
- Sales
- Pricing
- Processing of contracts
- Marketing
- Production
  - Production control / project management
  - Customer communication in projects and during production

A company which applies the templates described below is already equipped with the basic framework for a BIA adapted to SMEs if additional framework conditions, if any, were defined in advance. Now, only additional processes, if any, and their associated resources must be added. This brief BIA can also be the body for a complete BIA, in which the business processes and resources which are not supported by means of IT are also considered.

2.7.2 Damage scenarios

The classic damage scenarios include: financial effects, impairment of the ability to perform tasks, violation of laws and contracts, negative internal and external effects (damage to reputation). They are used to purposefully classify the effects of a failure. When doing so, SMEs should select the damage scenarios relevant for their respective company and consider these scenarios in the BIA. However, it must be taken into account that minor effects are subordinate to major effects. Thus, damage with massive financial effects is even high if the associated violations of contracts are only low.

2.7.3 Classes of Effect

The classes of effect are intended to facilitate the assessment of damage. For the assessment, this study recommends to determine qualitative classes of effect, since it is not always possible to predict an exact amount of damage or frequency of occurrence.

The following table shows a possible classification of the classes of effect (1 - Low, 2 - Medium, 3 - High, 4 - Very High). The presented values are only examples and the organisation applying them should by all means adapt them to its own understanding of a low to very high damage.
<table>
<thead>
<tr>
<th>Class</th>
<th>Quantitative description</th>
<th>Qualitative description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Low</td>
<td>The financial damage to be expected amounts to up to 1% of the annual turnover.</td>
<td>• The impairment of the ability to perform is negligible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is no threat to prestige / reputation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No violation of laws or contracts</td>
</tr>
<tr>
<td>2 – Medium</td>
<td>The financial damage to be expected amounts to up to 5% of the annual turnover.</td>
<td>• The ability to perform tasks is tolerable and the post-contingency tasks to be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>expected can be processed during normal daily business.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There are violations of laws or contracts with minor consequences. An escalation of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>these violations is not expected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In individual cases, the contingency is perceived outside the organisation. However,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>no consequences are to be expected due to this perception.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The impairment is assessed to be tolerable.</td>
</tr>
<tr>
<td>3 – High</td>
<td>The financial damage to be expected amounts to up to 10% of the annual turnover.</td>
<td>• The ability to perform tasks is impaired to an intolerable extent and losses in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quality of work or failure to meet deadlines must be expected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The post-contingency tasks to be expected can no longer be processed during normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>daily business. Post-contingency tasks can only be gotten through with additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>personnel or a lot of extra work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There are violations of laws or contracts with consequences to be expected (contractual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>penalties, action).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The contingency is perceived outside the organisation. The contingency is perceived by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a majority of the customers and</td>
</tr>
</tbody>
</table>
Class | Quantitative description | Qualitative description
--- | --- | ---
| | in the regional environment. | • The impairment is no longer assessed to be tolerable.
| 4 – Very high | The financial damage to be expected is clearly above 20% of the annual turnover. | • The ability to perform tasks has been interrupted severely. It is no longer possible to perform tasks.
| | | • The post-contingency tasks can no longer be performed in a reasonable manner.
| | | • Fundamental (grossly negligent) violation of laws or contracts with serious consequences. Very high contractual penalties or civil action against individual persons can be initiated.
| | | • Ruinous effects on the social or financial position.
| | | • The contingency is perceived very clearly outside the organisation. The contingency is perceived by virtually all customers and in the supra-regional environment.

Table 2: Example criteria of the classes of effect

2.7.4 Time Horizons

The assessment in different time horizons is intended to identify those business processes and their required resources which must be available again quickly. This makes it possible to purposefully initiate safeguards and set priorities. To keep the assessment effort within limits, it is recommended to define only three time horizons. The time horizons <1d, <3d and >3d have proven their worth in practice. If it is possible to identify in advance that high damage occurs when a resource or a process only fails for a few hours, it is recommended to add an additional time horizon (<4h). These time horizons are examples and must be adapted by the organisation to its requirements.

2.7.5 Determining the Maximum Tolerable Period of Disruption (MTPD)

The maximum tolerable period of disruption, also referred to as MTPD, results from the assessments of the expected damage in the event of a process failure and is the time frame in which the recovery has to be carried out to avoid serious damage. We recommend to determine the MTPD at the time at which the effect reaches the class "High".
2.7.6 Form to carry out an IT BIA

The following table constitutes an example of the recommended procedure of performing a compact IT business impact analysis. The following table is to be applied to each business process.

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does it have on the company when there is a failure of the core process?</td>
</tr>
<tr>
<td></td>
<td>Failure &lt;1d</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>What IT systems are absolutely necessary for an contingency operation of the process?</td>
</tr>
<tr>
<td>3</td>
<td>Which of the IT systems contain data which might not be recovered in the event of a loss?</td>
</tr>
<tr>
<td>4</td>
<td>Are there alternatives or alternative workflows to these IT systems?</td>
</tr>
<tr>
<td>5</td>
<td>What IT service providers are absolutely necessary for an contingency operation of the process?</td>
</tr>
<tr>
<td>6</td>
<td>Are there alternatives or alternative workflows to these IT service providers?</td>
</tr>
</tbody>
</table>

Table 3: Form to carry out the IT BIA

For this purpose, ask yourself the question: on which of your IT systems and IT service providers do the business processes depend directly? This allows you later to identify and implement the best possible business continuity strategy.

In the appendix of this study, an example of a BIA with typical assessments of the effects and free fields in which you can enter the IT systems and service providers can be found. We recommend to complete this form. A download link to the document can be found at [BSI_2013].
3 Business Continuity Management in Private Cloud usecases

Whereas services and applications in the public cloud can be accessed by the general public, the services and applications offered when using a private cloud are only available to a restricted group of users, typically only to the employees of a company. In most cases, the providers of private cloud services and their users belong to the same organisation, as the private cloud is often run by the organisation's own IT department. Compared to public clouds, private cloud services have the advantage that the security, configuration and operation of the offered solution are still in the hands of the organisation (usually as responsibility of the IT department) and have not been handed over completely to a service provider. As all components are run on-site in the computer centre of the company, higher levels of investment are of course involved when building up a private cloud, since the corresponding hardware, software and other infrastructure components must be purchased. These costs are offset by the benefits due to the dynamic provisioning of IT resources and, as described in this study, a higher level of availability. Therefore, these costs are assessed to be reasonable in many cases.

3.1 Private Cloud and Virtualisation

In this document, private cloud is also understood as using virtualisation technologies even if only two virtualisation servers are referred to and no entire server farm is required. Virtualisation software provides standardised resources (computing power, memory and hard-disk memory) irrespective of the real physical resource (the concrete processor, memory or hard-disk memory). Virtualised IT systems are thus no longer dependent on the concrete physical hardware. This solves many problems, as it is for example no longer necessary to purchase identical hardware following a failure. In many cases, it is no longer necessary to switch off the IT systems for repair, as it is, for example, possible to replace hard disks during live operation. Even apart from contingency planning, the advantages of virtualisation, especially virtualisation of the servers, are obvious: Thanks to an individual high-performance server, it is possible to provide several virtual systems on a single piece of physical hardware. At the same time, you should not forget that the replication associated with the virtual infrastructures requires bandwidth in the network. Accordingly, the bandwidth of the network must be dimensioned in such a manner that replications do not impair any other network traffic too much.

3.2 Contingency Prevention

In an environment with physical servers, concepts were and are distinguished between cold, warm or hot standby for contingency prevention. Here, a system identical to the productive system is built up in parallel and either switched off (cold standby) or kept in such a state that it can be switched on, but is not used (warm standby) or switched on and supplied with data whilst being mirrored synchronously (hot standby). Even if there have been no changes to this fundamental classification on how contingency prevention is implemented, the introduction of virtualisation has resulted in a different contingency prevention design.

Especially in areas of application requiring a high level of availability of systems, virtualisation is particularly advantageous and widely used. Due to the fact that virtual machines can be moved from one host to another during live operation, an enormous level of availability can be achieved using this technology. Using the high-availability module, the provided service is available to the user in the event of a system failure without any interruption. Here, the hypervisor performs a continuous in-memory replication to a machine run on another virtualisation host. However, this involves considerable costs for the software and the required Storage Area Network (SAN); therefore, SMEs instead usually make use of switching an image manually from a virtualisation server to one of the remaining servers.
The use of virtualisation for contingency prevention and response in SMEs is in most cases to run two or, in case of slightly larger IT landscapes also several, virtualisation servers. If there is an contingency, they replace each other. Where possible, the virtualisation servers are located in spatially separated areas with different power supplies and ideally in two different fire protection zones.

During regular operations, the virtual machines are distributed to all virtualisation servers and the images are replicated to the respective other virtualisation servers. By simply copying virtual machines, the entire state of the system including updates and patches is also backed up. Virtual machines are just files and could thus be backed up by simply copying them to one of the other virtualisation servers.

These descriptions include the concepts of cold, warm and hot standby. A hot standby is given when the virtual machine is synchronously mirrored on the other virtualisation server. In the event of a failure of one server, the other server takes over its tasks without any loss. If only the image is backed up at regular intervals, e.g. every hour, and can be started on another server, this would be considered a warm standby. If the image of the virtual machine is only stored at a single site and cannot be started up there, this is referred to as cold standby.

The daily backup of the entire image does not replace the backup of data in the image which is still required, but it ensures that guests can be started on the virtualisation server that is still available in case of an contingency. The administrator must start up the corresponding systems on the remaining virtualisation server when a malfunction is detected, i.e. perform a manual switching operation, which is usually completed within a few minutes.

Using virtualisation, it is thus possible to set up a proper restoration procedure for virtual systems together with the data stored on them without much effort and relatively quickly. In addition, if the required amount of work is taken into consideration, such a solution compare favourably to a classic cold standby solution (without virtualisation), as the non-virtualised replacement system must also be kept up-to-date constantly regarding the current configuration and patch state, which is carried out automatically when using a cold standby solution with virtualisation.

### 3.3 Multiple Sites

Another matter under consideration is the redundant design options of sites in SMEs as contingency planning and the problems occurring in this context. If a SME operates more than one site, there is already a good basis of redundant data storage with respect to contingency planning, as the systems are located in physically separated premises. The data can be replicated for all sites so that the same data is available to each site.

#### 3.3.1 Replication and Amounts of Data

Depending on the total amount of data which must be replicated amongst all sites, the bandwidth requirements also increase with a rising data volume. If the sites are only connected to each other via ISDN or a slow DSL line, the replication of entire databases will become a long-lasting undertaking, in particular if this no longer relates to only two sites. If it is required, for example, to synchronise the data of five sites to be able to compensate for failure of individual sites, the requirements to be met by the WAN connections of the individual sites increase, as such a "star-shaped" replication is very data-intensive.

There are various reasons why a broadband connection to the Internet and other sites is not available to a SME. On the one hand, the costs for a dedicated connection between several sites are relatively high and often do not pay off for smaller SMEs. Another reason is the fact that SMEs are often not based in urban areas, but frequently in more rural regions in which the availability of broadband Internet connections is sometimes still scarce. Thus, a reasonable replication of data between several sites within an acceptable period of time can no longer be realised due to weak upload and download rates. Due to high latency periods, such a synchronisation of databases is not achieved without considerable delays. In general, it must
be taken into account during the planning phase that the bandwidth does not only have to be designed for the backup, but also for the restoration to ensure that the intended Recovery Time Objective (RTO) can also be complied with. Thus, the work of mobile employees who have to access company and business data, for example using a VPN connection could only be carried out to a limited extent, in particular if the entire bandwidth provided was already used up by the implemented replication mechanisms.

A calculation example illustrates this problem. In this calculation, virtual systems were synchronised to a central provider:

<table>
<thead>
<tr>
<th>Upload bandwidth (Mbit)</th>
<th>Transmitted data (GB/h)</th>
<th>Average daily period of replication per VM (minutes)</th>
<th>Average daily replication rate (VMs/24h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.4</td>
<td>200</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>0.8</td>
<td>100</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>1.7</td>
<td>40</td>
<td>37</td>
</tr>
<tr>
<td>10</td>
<td>4.2</td>
<td>20</td>
<td>74</td>
</tr>
<tr>
<td>20</td>
<td>8.4</td>
<td>10</td>
<td>137</td>
</tr>
</tbody>
</table>

Table 4: Experiences with replications of the cloud service provider ACP Solutions (by courtesy of Thomas Reichenberger from ACP Solutions)

A solution for this dilemma is to use a virtual site, i.e. the installation of IT systems in the computer centre of a provider. Now, all sites synchronise and replicate only using this single virtual site with a high-bandwidth connection. Thus, the data cables are relieved, as each site now only sends and receives its own data and no longer the data of the other sites, too. Since, in this case, not only the organisation's own IT is used, but also an external offering, this case is a hybrid cloud application and is described in more detail in the following chapter.

3.4 Particularities of the Business Continuity Management Process

In addition to the provision of standardised resources based on different hardware, virtualisation or cloud technologies also change the contingency planning with the processes for business continuity, recovery and restoration and return to normal operation. Thus, the focus changes from the recovery and its planning to planning the manual switching operation of the guests from one virtualisation server to another or, ideally, to only planning the control of successful automatic switching operations. When using virtualisation, planning for the contingency operation is thus reduced to resource planning within the virtualised environment or to planning where on the business premises the hardware for the private cloud is installed. This applies at least to the servers.

Business continuity management for clients is also undergoing a radical change, since the same mechanisms as used for the servers are applied when distributing server-based computing and the thin client used for this purpose. If workplace computers, also referred to as fat clients, are still used, their replacement should be considered. The clients are no longer considered in this study.

3.5 Tests and Exercises

In virtualised environments, it is much easier to practise business continuity plans. The effects of dynamic distribution of resources as well as switching to the hardware in another room or at an external cloud provider can also be tested during normal operation. There is no need to prepare new plans, as standardised plans can be built on, for example for switching to another virtualisation server. The training and exercise effort in virtualised infrastructures is thus much lower than in physical infrastructures and therefore also possible for a SME.
4 Business Continuity Management using the Hybrid and Public Clouds

So far, only the effect of virtualisation technologies or the organisation's own cloud infrastructures to the business continuity management in SMEs have been considered. If, however, the cloud infrastructure of a public provider is used, there are additional effects on the business processes of a SME and its business continuity management. Since both the private and the public cloud are used together in this case, this is called a hybrid cloud.

Using public cloud models also results in advantages of standardisation. It is no longer important to ask for the concrete hardware, but only to lay down general requirements such as computing power, working memory and hard disk memory and availability.

Due to the outsourcing of services into the cloud of a professional provider, high availability periods and short duration of a data loss can be achieved in the event of a failure (Recovery Point Objective and Recovery Time Objective). At the same time, the confidential (encrypted) connection to the services is of vital importance when using these cloud services.

When taking the use of available cloud solutions into consideration, it is not only possible to outsource complete servers, but also office applications (Word, Excel etc.) and other applications to the data cloud. The best-known example is the provision of email services. Security-related services such as malware detection and virus scanners, too, can be outsourced to the cloud. At the moment, outsourcing the services completely into the public cloud is rather rare. A scenario that is encountered more frequently is the supplementation of the organisation's own services by offerings from the public cloud. For example, a backup at a second site was an expensive undertaking for a company operating only a single site. Today, each company can use cloud providers for this purpose. The following cloud computing options are available:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Security as a Service
- Remote Backup / Backup as a Service (BaaS)
- Disaster Recovery as a Service (DRaaS)

Using these cloud architectures, a company succeeds in reducing the operation of many central IT components. Only rarely will it be possible to detach completely from such infrastructures, as it usually still necessary that switches, firewalls and the VPN server in particular are available for the secure connection to the cloud provider. The advantage of outsourcing services completely into the cloud is the extremely high availability periods that can be achieved in this way. These statements apply with the restriction that a network for the connection to the cloud, power supply, infrastructure for the connection to the cloud provider and corresponding clients must, of course, be ready for use in the organisation.

4.1 Software as a Service (Saas) and Platform as a Service (PaaS)

Software as a Service and Platform as a Service are closely related offerings of cloud providers, as an already configured environment is rented in both cases. When using PaaS, an application software such as a web shop is installed on this platform, and when using SaaS, this application software is made available by the provider. From the perspective of contingency planning, there is no difference in this case, since a plan on how the company can still maintain its business processes even in the event of a failure of the provider should be available in both cases. Details on this aspect as well as on data backup can be found in the corresponding chapters.
From the perspective of contingency prevention, too, both offerings are fairly comparable. The reason for this is that all technical safeguards to maintain the service and to ensure recovery and restoration are the obligations of the provider. However, this does not release, as already emphasised, the management of the SME from contingency planning, it only changes the contents. In this respect, see also chapter 5 “Contingency Planning when using the Public Cloud” on page 32.

4.2 Disaster Recovery as a Service (DRaaS)

This relatively new offering on the constantly developing market is a combination of several technologies. In addition to the Backup as a Service and the virtual site, these offerings include the following services:

- Replication of data including hard disks of the virtual IT systems
- Environments prepared for the operation of the virtual IT systems
- Replacement systems for the physical IT systems
- Access and authentication for the employees

In the enterprise environment, the products used there offer the functions required for the replication of data and virtual IT systems. Thus, all providers of SAN and also the market leader in virtualisation technologies have already installed functions for the replication of large amounts of data even with high latency of the transmission lines, i.e. large distances and the low bandwidths of Wide Area Networks (WAN) as compared to computer centre technology. In most cases, these technologies cannot be projected as purchase costs in the IT budget of a SME. As not only a replication of data is offered in this case, but a complete concept, the assignment of a DRaaS is a complex project, in which the contractor must take into account all particularities of the contracting company. In most cases, the price charged by the providers for this service will exceed the IT budget of a SME.

For a SME, it is nevertheless possible to use the benefits of technological progress at reasonable cost. Thus, a virtual site can already be compared to DRaaS, because the capacities of the cloud provider are also used in this case to increase the level of reliability and reduce restoration times. In this case, however, no recovery of the physical IT systems will be carried out. The SME itself must also take care of the replication of data.

4.3 Virtual Site at the Provider

Here, the SME either rents the IT systems from the provider or installs its own hardware on the provider’s premises. These IT systems are then either used as backup for an contingency or they are used for processing daily and continuous business operations. If the rented systems are virtual systems, they are mostly referred to as Infrastructure as a Service.

A special form of this additional site is when the IT systems at the provider are used as central IT system for the replication between several sites. Then, all sites must only replicate with this site which is much better connected in most cases. Thus, the load of the data cables to the sites is reduced substantially.

For a SME, the virtual site offers several advantages, as the data centres of the providers have, in most cases, better protection against natural hazards such as fire, lightning and water than a server room on the SME’s own premises. In most cases, the connection to Wide Area Networks is also designed with multiple redundancies at larger providers. The power supply is purchased from several distributors and is secured by means of adequate UPS capacity and often also with additional power generation by means of contingency power generators. Then, the backup of the data is purchased from the same provider when such a site is built up. Thus, fast data transfers and short recovery times are ensured in the event of a failure of the IT systems at this site. In general, all these measures cannot be realised with the budget typical for a SME. A virtual site is usually accompanied by a higher latency period for the organisation’s own applications as compared to local operations. This aspect should be taken into account during the planning phase accordingly. If the resulting latency periods are too high, additional safeguards must be implemented, for
example, the organisation's own terminal server infrastructure for contingencies. In addition, it should also be ensured that the cloud provider offers all services that are specified by the organisation's own information security management. If, for example, data backups are carried out every day, then this service must also be offered at the cloud provider's virtual site.

If the IT systems are not integrated into ongoing operations and only held in reserve for an contingency, the recovery at a virtual site is generally more complex than at the organisation's own physical site and should be planned and tested carefully. If, for example, only a part of the IT infrastructure is backed up at the virtual site and is restarted from there in the event of an contingency, IP addresses and routing tables must generally be adapted. These adaptations may possibly be simplified or even become obsolete using technologies such as "Network Bridging". Such simplifications should be examined and assessed.

4.4 Remote Backup / Backup as a Service

The decision which backup strategy a company runs depends on the internally defined functional and operative requirements. In addition, a detailed security analysis, data protection as well as legal aspects when outsourcing partially sensitive business data also play, of course, a vital role of which the decision-makers must be aware. When these risks and general conditions have been sufficiently taken into account, companies can implement an effective and uncomplicated data backup strategy using the options provided by cloud computing.

When choosing a backup strategy, the following principle applies: The further away the data is from the operating system, the better. The backup requirements are defined by several influencing factors (see BSI IT-Grundschutz safeguard S 6.34 Determining the factors influencing data backup), i.e.

- Specification of the data to be backed up
- Criticality of the data/availability requirements
- Time and expenditure required for data reconstruction without data backup
- Volume of data
- Change volumes
- Modification times of the data
- Deadlines
- Confidentiality requirements
- Integrity requirements

Classic backup strategies include that the data of employees is stored on a centrally provided file server within the company. The data stored on the file server is subject to a regular data backup to ensure that data can be restored if necessary. Whether it is an incremental backup or a full backup of data is irrelevant for this consideration for the time being. However, the cooperation of the employees is required in the event of a centralised backup strategy to ensure that they actually store their data on the file server, provided that they are in the company network and can access the file server. If this is not the case, there is automatically a temporary storage of the data locally on the system. If data is not synchronised at the next opportunity, data can get lost if the hard disk of the client is defective. In contingencies, data can be reconstructed from the hard disk; the financial investment for such a restoration is only only justified for extremely critical data.

From the providers of online storage space available on the market, the company can select a product which meets the special requirements of the respective company. The pricing model depends on the respective service provider and can be performed according to the following criteria or a combination of these:

- Number of the total amount of data that is backed up
- Number of machines for which a backup is carried out
• Number of versions stored for each file
• Retention periods
• Service levels and provided functions

Probably the greatest advantage of an online backup is that the approach of storing the data at a sufficient distance to the operating system is implemented effectively. Since the backup files are stored physically in another geographical region in most cases, they are secure against fire, water or other disasters occurring at the actual site of the organisation. With regard to an SME, this is a particularly important improvement over the status quo, as file and backup servers are only rarely located in separate rooms and there is a trend to store systems in the same premises. If there was a fire, file and backup servers would be equally affected, which could result in a complete loss of data in the worst case.

Since the service providers' computer centres are equipped with better connections than the SME itself in most cases, it makes sense that every branch only transfers the data stored at its site to the online storage space. The data is thus consolidated at a central point, i.e. all databases of all sites are then stored in the online storage space. Thanks to this central hub, the obstacles that might result from a rather weak Internet connection are thus reduced. The bandwidth required for the replication of databases is reduced many times over as compared to a mutual replication of the sites.

Using a central hub also results in an enormous advantage for mobile employees. If they need to access data, they do not have to access them via the weakly connected site, but can use the central hub instead, which makes all databases available in a consolidated form and, at the same time, provides a better and probably also more reliable connection. In such a scenario, the only restriction is then the connection of the mobile employees and their systems.

### 4.4.1 Data Backup on the Client

In addition to the dedicated offerings for server storage capacities, there are also data backups for clients storing the data in the cloud regardless of the company's servers. If this solution is chosen, the company installs a program of the provider of the online storage space on the clients, which performs the synchronisation whenever Internet access is available. Whenever possible, the data should be encrypted prior to synchronisation. Additional information on the secure use of online storage space can be found in the IT-Grundschutz white paper on online storage space [BSI_2012c](in German only). Another advantage of the online storage space is the option to share the data with other employees, customers or the entire Internet. For SMEs, this option can replace the file server; great care, however, must be taken to ensure that the data is then only shared with the desired group of people. Studies at large cloud providers have shown that users share up to 30% of all files for far too large a group of people, often the entire Internet.

Almost all manufacturers of client operating systems also offer cloud storage in their core product. For example, data of any type and often of any amount can thus be stored in the cloud, also allowing access to this data using mobile devices such as smartphones. It is thus also possible to exchange the data between the employees without operating a separate file server.

Whereas the administrator has always been responsible for carrying out or restoring backups when the traditional backup method is applied, this responsibility is transferred to the user when using client-based cloud technologies. The administrator has less and less influence on which data is transferred to the cloud service provider. The only ones who can still exert influence are the data owners themselves, as they are able to define (depending on the product used) which folders have to be synchronised and which folders (e.g. highly confidential contents) are excluded from being synchronised. By implication, the users are thus responsible for the restoration of their data, as they can directly access their cloud account.

Here, the aspect of user friendliness which is achieved when backing up data in the cloud is significant. Due to the fact that the backup is carried out transparently for the user without being involved (after a one-time initial configuration), they can concentrate completely on the business processes without having to take the data backup aspect into account. If a file must be restored from the cloud storage, the user can extract the
required file from the online storage space. For a restoration, it is first necessary that the IT company restores the file for the user when a traditional backup method is used. Long wait times can be avoided by means of self-help possibilities.

4.5 Data Backup using IaaS and SaaS

As the hosts of cloud solutions are also responsible for the backup of data, the person responsible of a SME no longer has to take care of the preparation of a data backup plan and the performance of the backup of individual systems when using services in the public cloud, as this discipline of contingency planning is outsourced to the respective host of the cloud solution. Defining the protection requirements, however, is still necessary to be able to select providers and their offerings. The computer centres of large providers are often designed with multiple redundancies and are subject to continuous synchronisation/mirroring so that damage events rarely have a noticeable effect on the business process of a SME. Employees of the SME can continue to work, regardless of whether there was a power failure in a computer centre of the cloud provider.

In case of a loss of data, the cloud provider is responsible for the restoration of backups and not the SME itself. Each safeguard of the business continuity management is transparent for the SME; thanks to the implemented continuity strategies of the cloud provider, the availability of systems and data is ensured. However, the SME thus depends to a large extent on the proper functioning of the cloud provider’s contingency planning safeguards insofar as a concrete failure scenario occurs at the cloud provider. If all implemented continuity strategies fail, the SME is no longer able to work either. As a cloud service provider of SaaS only provides a special service in most cases anyway, there is at least a certain degree of risk distribution in this respect. For example, often just one business process is completely or partially affected by a failure in the event of a failure of a service provider. When applying IaaS, a provider is used for all services in most cases. In this case, a failure results in serious consequences for the business processes.

At this point, it should also be noted again that losses of data can also occur at service providers, which is why additional security safeguards must be implemented within the framework of an alternative backup strategy for very business-critical data in particular. In practice, this additional safeguard is in most cases a regular, e.g. weekly download of data to the organisation's own data medium stored in a fire-proof data cartridge on the premises of the SME.

4.6 Technical Personnel with Cloud Authorities

Another aspect that has to be mentioned when using such services is the need for specialised IT personnel. For example, the provision of email services via Microsoft Exchange is a complex undertaking and should only be carried out by persons who are familiar with the configuration and operation of mail servers, since ignorance would also result relatively quickly in failures of the mail system due to misconfigurations. The same applies to the private and public cloud. With respect to SaaS in particular, the employees no longer have to know in detail how the servers are operated, but the connection of this service to the local IT systems, the dependencies between the services and the changed troubleshooting methods are challenges which the employees commissioned with the IT operations have to face. Depending on the extent of the chosen outsourcing of IT operations to the cloud, the SME can partially reduce the need for IT personnel, but must take into account the necessary authorities for complex relationships with service providers and also business partners, if any, with regard to employees.

4.7 Internet Connection of the Business Premises

Using cloud services requires a permanent and fast Internet connection to allow the smooth transmission of data and thus adequate operation. The SME’s bandwidth to the Internet must always be taken into account as a limiting factor. In urban areas, the connection to the Internet is often fast and reasonably priced,
whereas it is often not possible to be provided with a sufficiently fast Internet connection in smaller cities and particularly at sites outside villages or towns. However, this connection can also be interrupted at any time by a damage event for short or long periods of time.

In addition to the availability of the network connection to the cloud service providers, the confidentiality of this connection is also indispensable. For web services, a HTTPS connection must always be available. For the secure connection of server services or client images, an encrypted VPN connection must be established. Special attention must be paid to key and certificate management. Further information on VPN can be found in IT-Grundschutz module 4.4 of the same name. Organisational and planning safeguards on key management can be found in IT-Grundschutz module “1.7 Crypto-concept”.

With some cloud solutions, it is also possible to continue to work temporarily without a connection to the provider, as the client stores the data to be processed locally and synchronises changes using the public cloud service. Synchronisation takes place as soon as the connection is available again. Thus, it is possible to compensate for network failures, but ultimately there is the disadvantage that it might not always be possible to access all data or their latest version. Examples of such services are mail, data backup and replication services as well as the virtual site described above unless it only supplements one IT system in the branch office and does not replace it. These mechanisms are also only able to compensate for the failure and to allow the employees to carry out their work only for a limited period of time.

For contingency planning, it is therefore necessary to take into consideration the internal networking in the office as well as the connection to the Internet and to define and establish corresponding safeguards ensuring the availability of the connection to the Internet. In many cases, a mobile connection is already available to employees, as described in the next chapter. When using SaaS, IaaS and the virtual site, these employees then remain able to carry out their work. In order to also supply the other office workplaces with a redundant connection to the Internet, a router with a built-in UMTS modem as backup is a frequently used method ensuring at least that the services that can only be accessed via the Internet are still available. If a site is lost, such a router can also be set up quickly in another site so that a precaution for workplaces and their supply with an Internet connection is also included in the business continuity plan.

4.8 Mobile Connection to the Public Cloud

Due to the possibility of a mobile connection to a public cloud, the matter under consideration is extended significantly with respect to the business continuity concept. If mobile IT systems are available to the employees or if they are allowed to dial in to the public cloud from their PCs at home, business processes for SMEs can be protected against the failure of the building even at a reasonable price. All business processes that are run in a public cloud can thus be protected against failure or recovered in such a short period of time as would never be possible without cloud technology.

This only applies to all services which are directly obtained from the public or hybrid cloud. When IT systems operated by the company on its own premises are used, the company can only utilise this advantage if these IT systems are also secured in the hybrid cloud within the contingency planning framework. Thus, an IT system at the virtual site can take over the tasks of a failed IT system at a site that was, for example, destroyed by a fire almost without any problems and immediately provide the employees with the required services thanks to a mobile connection to alternate workplaces.

4.9 Authentication

All services used via the Internet have the advantage that the employees can access these services from anywhere. At the same time, however, this results in a security problem, as it is associated with the risk of unauthorised access by third parties. As a result, the authentication of the employees is of particular importance. It is thus absolutely necessary to use adequately complex passwords and to also change them at regular intervals or, even better, to use a stronger authentication procedure. Since even former employees without access to the premises of the company and to the offices can still access the services in the cloud in
an unimpeded manner, it is particularly important to also block the accesses to the services upon termination of employment.

4.9.1 Two-Factor Authentication

The processing of data with higher protection requirements also requires a higher level of protection. Examples of such data are data about natural persons subject to data protection and confidential data of the company which is of particular importance for the business. This data can be, for example, calculations, building plans or customer data. To process such data, it is recommended to only use services with additional methods for authentication. Unfortunately, only a few providers offer two-factor authentication. In addition to the first factor, the password, the second factor is something the user possesses. This can be a token generating quasi random numbers at the touch of a button and using them for authentication. Methods that are available on the market and suitable are as follows:

- GridCards
- Certificates
- SMS tokens
- OTP tokens as software or hardware

If two-factor authentication is used due to the high protection requirements of the information, then the cloud service provider must also provide this protection and it must be ensured that the tokens are available at the service provider and the recovery is thus not delayed unacceptably.

4.10 Selection of the Cloud Provider

The actual focus of the business continuity management changes following the outsourcing of components and services into the cloud. Whereas ensuring availability by means of continuity strategies of the company's own hardware was the top priority of the business continuity strategy, the main focus is now placed on the selection of a suitable provider, as the offerings are standardised and can only rarely be adapted. Contractual arrangements beyond the selection of an offering cannot be implemented realistically in practice at least with larger providers. To be able to assess a provider, certifications also play an important role, for example the "ISO 27001 auf der Basis von IT-Grundschutz" certificate and, if the availability of the service provider is concerned in particular, the certificate of the business continuity management in accordance with ISO 22301. If such certificates are available, they must include the part of the service provider, in which the desired services are rendered and, if corresponding high security requirements have to be met in the SME, providers certified accordingly should be preferred.

The advantages of a strategic decision in favour of cloud computing seem to outweigh the disadvantages, but there are still several factors that have to be taken into account before choosing the cloud solution. As fantastic as the realisable availability periods and the low probability of a failure when using the cloud might sound, there are still some central questions which every managing director of a SME should ask themselves:

- What do I do if my cloud service provider fails and how do I ensure the availability of my business process?
- How long is the period of time that is acceptable for the company when data cannot be called temporarily?
4.10.1 Taking the criticality into Account

A business impact analysis is also required to be able to identify critical business processes. The results of the BIA should be used as the basis for the selection of the appropriate cloud provider and the contractual agreement. In this respect, only providers offering an adequate level of automation of the recovery processes come into question for very critical business processes. This must be examined closely on a case-by-case basis.

4.10.2 Interface to Business Continuity Management

The public and hybrid cloud providers take over many aspects of contingency planning for the processes of the SME. The data backup of the images or the individual files is specified within the contract and thus no longer has to be carried out by the SME itself. At the same time, it is always also necessary to ask for the contractual penalties or other negative effects for the provider if the contract is not adhered to. For example, offerings using the service for six months free of charge might seem to be attractive, but if important data is lost, this is still very harmful to the SME. Therefore, all data should also be backed up additionally by the SME on its own systems, e.g. a data medium in the company's own office, as otherwise a total loss might occur in the worst case.

In addition to the technical requirements, data protection aspects for the business continuity management using cloud technologies are also an important planning aspect. Details can be found in the Eckpunktepapier of the BSI [BSI_2012a] and in the chapter "Data Protection and Cloud".

4.10.3 Provider Availability

To avoid the risk of a complete standstill in the event of a service provider failure, care should be taken when selecting the service provider that they guarantee a high level of availability and have also kept this promise in the past. The longer a provider is on the market, the more the risk that the provider will become bankrupt can be excluded. It is also possible to rely on a certain degree of risk distribution, i.e. not to have all services rendered by a single service provider. Thus, it could be ensured that not all business processes are similarly affected in the event of a failure. Some large providers offer the operation of the applications in different availability zones that are independent of one another and thus already contain a distribution of the failure risks. In addition to the specified support time (e.g. 365x24x7), it is also important for the assessment of the availability of the provider which RTOs and RPOs are offered by the service provider. It can also be advantageous if the provider offers a self-service portal by means of which the SME itself can initiate and monitor necessary recovery steps.

Another aspect to be taken into account when choosing a service provider is the geographical location. This aspect is important when considering data protection aspects. However, a SME should also think of the defence against industrial espionage by foreign intelligence services. When using cloud services in other countries, the legal framework of the respective country applies. In case of questions on the defence of industrial espionage, the SME should contact the constitution protection office of the respective federal state or the Federal Office for the Protection of the Constitution.

In addition to these aspects, it must also be ensured when assessing the geographical location that the support times of the helpdesk there are compatible with the company's main business hours.

Authentication, too, must take into account the security of the processed data. If, for example, data requiring special protection is processed, the provider of a service should also support additional methods such as tokens in addition to the usual user names and passwords.
4.10.4 Medium-sized Partners for the SMEs

In addition to the large providers of cloud services, smaller and medium-sized IT service providers are often also important partners for SMEs. They are often more flexible when it comes to their services and their personnel also supports the company on site. Thus, the IT service provider can not only take over the operation of a virtual site, but is also possible to assign this provider the operation of the IT systems in the company's own branch offices and to produce synergies. Moreover, the data protection problems occurring when personal data is processed outside Germany or the EU are also avoided by using a local cloud service provider. Furthermore, a SME should bear in mind the risk due to industrial espionage, which is significantly higher outside Germany and more difficult to prevent than within Germany. Regarding any questions on how a SME can defend itself against industrial espionage, it should contact the constitution protection office of the respective federal state or the Federal Office for the Protection of the Constitution.
5 Contingency Planning when using the Public Cloud

Due to an intensive use of cloud services, the company must thus only prepare itself for those contingencies affecting the company's own personnel, the client systems, the internal IT networking, the Wide Area Networks (internet service provider), the premises or the cloud service provider. Taking the threats of the BSI into consideration which are assigned to module 1.3 "Business continuity management", the consideration of the following threats should be essential for business continuity management when outsourcing to the cloud:

- T 1.1 Loss of personnel
- T 1.2 Failure of IT systems - only clients and components still hosted on site
- T1.10 Failure of a wide area network

Within the business continuity management framework, however, all failure scenarios actually affecting the SME must now be considered. The following table provides an overview of the possible failure scenarios that must be taken into account for the business continuity management process when the applications and services of a SME are outsourced completely to the cloud:
<table>
<thead>
<tr>
<th>Failure category</th>
<th>Matter under consideration for the business continuity management process</th>
<th>Matter not directly under consideration</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Failure of the building / infrastructure | • Data connection / Internet connection  
• Internal networking (if any) | | For the use of cloud services, an efficient high-performance and redundant WAN connection is a critical requirement. Failure scenarios that might occur during mobile operation must also be taken into account in the business continuity management process. |
| Failure (lack) of personnel | • Illness  
• Pandemic  
• Accident / death  
• Strike  
• Demonstration | | The overseeing of personnel is still completely in the hands of the SME and must always be taken into consideration in the business continuity management process. |
| Failure of IT computer centre | Only those critical systems and infrastructure components that are still operated directly on site in the SME must be taken into consideration. | System malfunctions or failures of IT systems that are operated at a service provider are no longer a direct matter under consideration. However, it must be taken into consideration which steps need to be taken if an improbable total failure of the service does occur at some point. |
| Failure of service providers | Failure of the cloud service provider (both in the short term due to a contingency at the service provider and in the long term due to bankruptcy) | Maintenance and service contracts with hard- and software suppliers no longer have to guarantee next-business-day delivery. In the case of hardware contracts in particular, the provisioning times of spare parts for server systems no longer have to be defined hypercritically. |
Contingency Planning when using the Public Cloud

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Matter under consideration for the business continuity management process</th>
<th>Matter not directly under consideration</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Business continuity management should rather focus on client systems.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Failure scenarios of the business continuity management and corresponding reactions for a SME
Data Protection and Cloud

Data protection is not the central focus of business continuity management, but special attention must be paid to data protection when using cloud services. Whereas data control is still in the hands of the company with private cloud computing, all data control is given up when using a public cloud. Registration for a public cloud service is performed quickly. However, if you try to obtain information on the precautions implemented to ensure data protection at the service provider, this is a difficult undertaking in most cases. Often, you can only guess which data protection precautions have actually been established by the service provider. The aspect of data protection in particular is more complicated in this case, as there is no possibility to exert any influence on how the data stored is handled by the cloud provider.

First, the company must know if the data that is transferred to the cloud service provider is subject to the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), which can be assumed in most cases. This is the case when the data contains a reference to persons, when the data is used for identification or allow inferences to be made about certain natural persons. Information on the financial situation, religious beliefs and political opinion of a person is subject to special protection requirements according to the definition of the BDSG. This can be customers', employees' or suppliers' data. Using personal data in the cloud is subject to the requirements of the commissioned data processing and may only be carried out within the European Economic Area (EEA) or in a US-American company with a valid Safe Harbor certification [LDI_1].

In the Eckpunktepapier of the BSI [BSI_2012a], illustrating security recommendations for cloud computing providers, the commissioned data processing in the cloud is addressed more explicitly:

"With commissioned data processing, the cloud user as client is still responsible for data protection without any restrictions. In terms of data protection, the cloud user still has full data control. In general, the commissioned data processing is not bound to any other material requirements; but a number of formal requirements must be implemented. The commissioned data processing requires a written agreement that must at least include the aspects listed in § 11 Para. 2 BDSG. The cloud computing provider as contractor is subject to the instructions given by the cloud user and is not allowed to decide upon the processing and use of the data independently. Prior to the start of data processing and afterwards at regular intervals, the client has to convince themselves that the contractor complies with the technical and organisational safeguards. This does not necessarily need to be checked on site, but can also be tested by independent bodies."

The storage location is another aspect that has to be taken into account especially when drafting contracts on commissioned data processing. “An important perquisite is that the data is only processed within the European Economic Area (EEC), i.e. within the EU as well as in Iceland, Liechtenstein and Norway. Only then is the cloud provider given a legal status that is comparable with an internal computer centre of the company [IX_2012].

Transferring non-personal data into the cloud is much easier. When considering the outsourcing of data to the cloud, the cloud user must still examine if this is really in the interest of the company. If it is data requiring particular protection that contains, for example, sensitive company information, a public cloud service should possibly not be used or additional safeguards, such as encryption, should be taken.
7 Scenarios for Contingency Planning in SMEs

In this chapter, three selected scenarios are used to illustrate how cloud computing or the intensive use of virtualisation technologies influence the business continuity management process. The following scenarios were selected, as it is assumed that they will occur more often in the near future. For example, a representative survey conducted on behalf of BITKOM and KPMG, an auditing company, among 436 companies showed that more than one third (37 percent) of all companies in Germany have already used a form of cloud computing in 2012, most of them with positive experiences (cloud monitor 2013).

The focus of the individually described scenarios is to consider the advantages and disadvantages of the cloud services in practical use when protecting critical business processes.

7.1 Scenario 1: All Applications in the Public Cloud

In this scenario, an engineering office with primarily mobile employees is considered. A dedicated office, in which all employees can be accommodated permanently, is not required due to the employees' high level of mobility. In most cases, they are at the customer's site. Instead, only a limited number of workplaces and broadband access to the Internet are provided in the business premises which the employees can make use of, if necessary, for meetings etc. All business processes are supported by Software as a Service offerings.

To carry out productive process, each individual employee only needs their laptop with an Internet connection to use the corresponding cloud services.

Due to the large number of cloud services offered on the market, only a selection of cloud services which are fundamental for each company and without which no company can be operated is considered in this scenario. Examples of such services include:

- Personal Information Management (PIM)
- Office solutions
- Central file storage and
- Virus protection.

As an example, the PIM service will be discussed in more detail. A PIM service makes the essential functions for the address, calendar, task and notification management available. Normally, this term suggests technically a complex Exchange infrastructure that can be used in the form of an Outlook client installed on the employees' notebooks.

If, however, the company wants to operate its own exchange infrastructure, the purchasing of additional hard- and software components as well as the corresponding technical know-how is required to realise this step. Furthermore, setting up an Exchange infrastructure requires a corresponding Active Directory infrastructure. The use of spam filter and virus protection gateways should also be taken into account. As mentioned above, personnel trained accordingly is required for the operation of such components, their maintenance and also corresponding troubleshooting. Another aspect is the time needed to set up the infrastructure at the company's own premises. The secure accommodation of the components in a suitable server room, in turn, places demands on the physical condition of the building and also requires an adequate power supply as well as suitable air conditioning.

The implementation of a data backup meeting the protection requirements of the data would also be very complicated, as there is a concrete dependency on hardware, software and corresponding personnel in this case. A failure of the building (e.g. failure of the power supply) would have an immediate impact on the employees, since the PIM and storage services are also run there and would be affected adversely or fail completely in an contingency. The creation of redundancies (power supply, hardware, air conditioning) for critical infrastructure systems is out of the question for the engineering office due to the costs incurred.
Using a cloud-based PIM service, the engineering office is able to free itself from the complex IT infrastructures described above, as required, for example, by Exchange. The time frame for introducing a corresponding cloud service productively is also shorter as compared to an in-house implementation.

Using the cloud-based PIM-service results in the following advantages for the engineering office:

- Relieving the strain on IT personnel,
- Ensuring reliability and adequate backup strategies from the service provider (e.g. redundant computer centres),
- Provision of resources based on need.

Even a failure of the company's own building is not critical for the employees of the engineering office, as only the accounting department is located there, whose critical period of disruption was defined in the BIA (business impact analysis) to be three days. The access to the PIM services and the cloud data storage is still possible in the event of a failure of the building and ensures that the employees remain able to carry out their work.

In addition to the PIM services, all other services can also be outsourced to the cloud. There are several offerings for Office applications on the market, which also include the backup of data and the joint work. Backing up the data on the laptops is not necessary, because all user data is synchronised by means of a storage service. The employees can restore or recover the data themselves as soon as their new notebooks are available. The notebooks are protected by means of virus scanners included in the PIM solution and a proxy of a cloud provider monitoring the HTTP traffic for malware is installed on the notebook.

In the course of the company's own contingency planning, it was ensured that the employees receive a new laptop from the IT support within a specified period of time. The cloud service provider is responsible for ensuring the availability and integrity of the data which the employee has stored in the cloud.

The business continuity strategy of the engineering office includes concluding corresponding Service Level Agreements (SLAs) with the cloud service provider, in which the availabilities of the offered services are specified within the contracts.

### 7.2 Scenario 2: Private Cloud and Backup in the Public Cloud

In this scenario, a SME operating a single site is considered. The company already operates its own IT infrastructure and is relying increasingly on server virtualisation. The company runs a total of two virtualisation servers in two separate IT rooms. The virtualisation server hosts all business-critical server applications. To meet the backup requirements, the company has decided to outsource the backup of all company data to a public cloud and is thus using the service of a specialised cloud service provider.

Within the business continuity management framework, the continuity of the critical processes (e.g. in the event of a failure of a room) is ensured by distributing the virtualised servers to the two virtualisation servers. The virtual servers required for the critical business processes are stored on the two servers resulting in corresponding redundancies. Thus, one of the two virtualisation servers acts as master for one half of the virtual machines while the other assumes the role of the slave for these virtual machines. The other half of the virtual machines considers this server to be its master and the other server to be its slave. During normal operation, the virtual machine is run on the master. If there is a failure of a virtualisation server or if the corresponding part of the building can no longer be accessed, the important server services and virtual machines are started on the virtualisation server that is still ready to operate.

The data of the virtual machines on the different virtualisation servers is synchronised by copying the virtual machines from master to slave every hour. Only the data which has been created or changed since the last copy operation of the virtual machines is not yet on the slave system. This data is lost if the master is lost. Here, it is important to allow a sufficiently fast synchronisation to ensure that the time at which the last copy was created is not too long ago.
In this imaginary company, contingency tests have shown that the switching process from master to slave is carried out in less than 5 minutes, which the management of the company considered to be sufficient. This short period of time is possible, since the company decided to purchase corresponding products performing the switching operation automatically. The software starts the machines automatically and provides them with the corresponding IP addresses as soon as a problem with the master system has been detected. Based on the criticality of the systems, the administrators have defined the priorities of the individual virtual machines. In the event of an contingency, the software starts the more critical virtual machines in a targeted manner. A manual switching operation is also possible and used for regular contingency tests.

The procedures required for the manual and automatic switching operations have been documented by the company in a business continuity handbook to ensure that they can be carried out by the personnel available in the respective contingency. The business continuity handbook describes in detail how any systems, including the virtualisation servers and the virtual machines, can be put back into operation on the slave. It also describes test procedures to verify that the services still function as desired.

Although the risk of a total failure of both virtualisation servers seems to be rather low, the company has dealt with this possibility and taken corresponding precautions within the business continuity management framework.

Thus, the introduction of an expensive backup solution in the company was deliberately opted against and, instead, the backup of all virtual server images was outsourced to a public cloud. A backup product allowing the outsourcing of entire virtual machines into the cloud is used. The images are uploaded automatically at defined times. Due to the configurable encryption, it is ensured that no unauthorised parties can access the data within the virtual image. Due to intelligent compression algorithms and the fact that only changed data is transferred, the time required for uploading the virtual image is reduced significantly. Finally, the compression also has an effect on the costs for the cloud storage. It is also possible to manually copy the virtual images or backups into the cloud, but the IT administrator themselves must then take care of the encryption.

If both virtualisation servers or the entire building are lost, a backup of all server images that can be installed and started either on the new virtualisation servers that have been purchased or at an contingency site is at least available from the public cloud provider.

As an contingency site, a cloud can also be used in this case. Thus, the time period until the company has again purchased functioning hardware for the operation of the virtual machines can be bridged. The company has also prepared itself for this situation. If an contingency last more than three days and if both servers are lost permanently, the images are encrypted after the keys have been handed over to the provider and started in a virtualised environment.

Without using virtualisation, the recovery would take several hours (or several days or weeks if both servers and the building are lost, as otherwise a complete new installation of the systems would be required, which would be associated with considerable additional time and expense. In addition, the business data would still have to be restored from the corresponding backup (if any), which would also result in temporal impairments. Here, the manual switching operation in less than half an hour is a considerable improvement. If all data was lost, it would be highly probable that the company would have to discontinue its business activities prior to the introduction of the off-site backups. This risk could be reduced significantly using the cloud service at very low cost.

7.3 Scenario 3: Additional Site in the Cloud

This scenario describes a SME with two sites which, due to their location in the business parks of two smaller villages, are only provided with a slow Internet connection. The users of both sites are involved in critical business processes, which is why the employees of both sites need to have access to the applications provided at the other site. The access, however, is mainly carried out on the server at the site on which they are working. Quick outsourcing or even mirroring of the data or applications between the sites cannot be realised due to the limited bandwidth, as the load on the cables would then be too high.
To improve the workflow and the contingency planning, the SME has rented a server from a German cloud provider and now mirrors the virtualised IT systems at this site at night when no employees are working. Synchronisation is faster, as the data now only has to pass one cable of a site, and is thus also possible with a low data transmission rate of the data cables at the sites. If one or both sites fail, the administrator can start the applications at this additional site in the cloud in just a few minutes and the data is not older than a day. The loss of a day's data was assessed by the owner of the SME as an acceptable risk.

Due to this structure, it is possible that all employees can continue to work from their regular or other workplaces even in the event of a loss of one or both sites. Thanks to this architecture, they are not necessarily bound to a specific site, since only an Internet connection with a corresponding bandwidth is required to be able to access the application. In the event of a failure, they can thus continue to work either from contingency workplaces at a site or using home office. For the home office, a VPN access, which they use in such a case, was installed on the notebooks for the employees.

As it has been contractually agreed upon with the cloud provider that the cloud provider also carries out the backups of the application, the SME is protected against data losses and stores a copy of the data in the locker of its respective bank branch, just to be on the safe side. For the SME, a hardware failure at the provider does not have any consequences in most cases, since the provider has implemented the corresponding business continuity strategies and, among other things, has created sufficient redundancies to ensure that the SME's employees can continue their work.
8 Conclusion and Outlook

So far, virtualisation and cloud technologies have often only been considered as technologies with a high savings potential and enormous challenges to information security. The major advantages offered for the protection of business processes against failure or for a rapid recovery with a reduced contingency capacity which can result from using these technologies, have not been examined extensively.

In addition to the technical aspects, such as the possibility of an immediate take-over in the event of an IT system failure, the advantages offered by these technologies are above all the lower costs as compared to redundancy concepts without virtualisation or cloud technologies. As outlined in this document, this advantage can be of importance for SMEs in particular, since this group of companies only very rarely operates a comprehensive business continuity management. As shown in this paper, these companies can achieve an unprecedented and previously unaffordable level of availability and protection against data loss thanks to virtualisation and cloud technologies. Using the aids to carry out a BIA outlined in this document, at least a rudimentary business continuity management can be established in SMEs, which might be the starting point for a more comprehensive business continuity management.

Despite all the advantages of higher availability that can be achieved more easily, it must not be neglected that many important questions of information security and data protection need to be answered prior to using cloud computing. Especially when the cloud service provider is based in a foreign country, questions on the defence from possible industrial espionage also need to be answered.

Deepening the trust in the reliability and confidentiality in cloud computing is an important task for the future. Only with secure cloud computing, will it be possible to make comprehensive use of the full potential of this technology.
9 Appendix: Example of an IT-BIA of a SME

Most SMEs should be able to apply this example of a Business Impact Analysis in this form.

9.1 Financial Accounting

This business area includes:

- Payroll accounting
- Invoicing
- Taxes, especially turnover taxes
Appendix: Example of an IT-BIA of a SME

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does a failure of the core process have on the company?</td>
</tr>
<tr>
<td></td>
<td>&lt;1d</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>What IT systems are absolutely necessary for an contingency operation of the process?</td>
</tr>
<tr>
<td></td>
<td>Workplace PC with word processing and printing option</td>
</tr>
<tr>
<td>3</td>
<td>Which of the IT systems contain data which might not be recovered in the event of a loss?</td>
</tr>
<tr>
<td></td>
<td>Central accounting server SXVRV013</td>
</tr>
<tr>
<td>4</td>
<td>Are there alternatives or alternative workflows to these IT systems?</td>
</tr>
<tr>
<td></td>
<td>Invoicing first using word processing; follow-up registration in the accounting department</td>
</tr>
<tr>
<td>5</td>
<td>What IT service providers are absolutely necessary for an contingency operation of the process?</td>
</tr>
<tr>
<td></td>
<td>None</td>
</tr>
<tr>
<td>6</td>
<td>Are there alternatives or alternative workflows to these IT service providers?</td>
</tr>
<tr>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

9.2 Distribution

This business process includes:
- Sales
- Pricing
- Processing of contracts
- Marketing
<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does a failure of the core process have on the company?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failure &lt;1d</th>
<th>Failure &lt;3d</th>
<th>Failure &gt;3d</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does a loss of data have on the company?

<table>
<thead>
<tr>
<th>Loss</th>
<th>Partial Loss</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Partial Loss</td>
<td>High</td>
<td>Very high</td>
</tr>
</tbody>
</table>

2   | What IT systems are absolutely necessary for an contingency operation of the process?  

*Workplace PC with word processing and email communication  
Email server with Internet connection*

3   | Which of the IT systems contain data which might not be recovered in the event of a loss?  

*Email server*

4   | Are there alternatives or alternative workflows to these IT systems?  

*Web mail accounts to send out offers*

5   | What IT service providers are absolutely necessary for an contingency operation of the process?  

*Web mail provider*

6   | Are there alternatives or alternative workflows to these IT service providers?  

*In general, changing to another web mail provider is possible for a short time.*

### 9.3 Production

This business process includes:
- Project management
- Customer communication in projects and during production
Appendix: Example of an IT-BIA of a SME

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does a failure of the core process have on the company?</td>
</tr>
<tr>
<td></td>
<td><strong>Failure &lt;1d</strong></td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>

What effects (1 - Low, 2 - Medium, 3 - High, 4 - Very high) does a loss of data have on the company?

<table>
<thead>
<tr>
<th>Low Loss</th>
<th>Partial Loss</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>High</td>
<td>Very high</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>What IT systems are absolutely necessary for an contingency operation of the process?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None (communication by phone and personal communication is sufficient)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Which of the IT systems contain data which might not be recovered in the event of a loss?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>Are there alternatives or alternative workflows to these IT systems?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>What IT service providers are absolutely necessary for an contingency operation of the process?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>Are there alternatives or alternative workflows to these IT service providers?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

9.4 IT Systems and Providers requiring Special Protection

It has proven useful to maintain an overview table of the critical IT systems and providers which quickly result in damage in contingencies.

<table>
<thead>
<tr>
<th>IT system</th>
<th>MTA</th>
<th>Effect in &lt;1d</th>
<th>Effect in &lt;3d</th>
<th>Effect in &gt;3d</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace PC</td>
<td>3 days</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Email server</td>
<td>3 days</td>
<td>Low</td>
<td>High</td>
<td>Very high</td>
<td>Web mail service</td>
</tr>
</tbody>
</table>
References

BSI_2011a  Bundesamt für Sicherheit in der Informationstechnik: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen;

DI_2012  Dell: Der Umgang mit veränderten IT-Anforderungen;

BSI_2012a  Bundesamt für Sicherheit in der Informationstechnik: Eckpunktepapier - Sicherheitsempfehlungen für Cloud Computing Anbieter;

BSI_2012b  Bundesamt für Sicherheit in der Informationstechnik: Webkurs Notfallmanagement auf Basis von BSI-Standard 100-4;

BSI_2008  Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4: Notfallmanagement, Bundesanzeiger Verlag m.b.H., 2008, 978-3-89817-693-4,

BSI_2012c  Bundesamt für Sicherheit in der Informationstechnik: Überblickspapier Online-Speicher;

LDI_1  LDI: Wie wird der Schutz der Persönlichkeitsrechte bei der Übermittlung von Daten in das Ausland gewährleistet?;

http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html