Guideline

Business Continuity Guideline

Version 3.0

June 1, 2019

AEB

Content

Companies using AEB solutions for managing and monitoring their logistics and global trade processes can rely on quality, operation and data security as well as on the failure resistance of the offered IT services.

AEB employees not only strive to guarantee smooth processing of our services, but also provide for the risks of emergency cases: Where can disruptions occur and how can protection concepts be optimized? Which precautions and measures must be taken to immediately restore system availability in case of a highly improbable partial or complete system failure?

The AEB Business Continuity Policy describes the specifications and the scope for implementing continuous operation at the top level.

Internally, additional documents such as the **Emergency Planning Concept** and the **Emergency Manual** support the implementation of an effective Business Continuity Management.

The **Emergency Guide** transparently regulates processes and responsibilities also for emergencies and disaster recovery. This means that also in the worst-case scenario, you can trust that the overview is maintained and AEB services will be available again quickly and professionally.

To ensure business continuity and maintain a high service level, we've taken technical and organizational measures (as outlined in Art. 32 GDPR) that are expressed in our **Security Concept**.

Remarks:
AEB has developed this policy based on the **Federal Office for Information Security** (BSI)'s standard component (100-4) on emergency management and the **ISO standards** ISO 22301 and ISO 22313.

Some internal details regarding the organizational and operational organization, corporate processes or technical details cannot be published due to security reasons. Therefore, this document provides a structural overview of the respective areas at AEB.

1 Scope

Our emergency management, which is referred to as **Business Continuity Management (BCM)** in the following, applies to our whole company. A key focus lies on the maintenance of the offered cloud services for our customers.

2 Who is involved in Business Continuity Management?

A high level of integration of the employees involved in the processes in IT, infrastructure, and services including data center operation is important to us. Therefore, no separate organizational structure resulted from the BCM concept. At AEB, dealing with BCM as a part of risk management is a **self-evident obligation for corporate management**. Therefore, we see Business Continuity Management (BCM) as being closely interlinked with our **ISO 27001**-certified information security management system (ISMS). There, BCM is defined as a separate regulatory area.

The following key roles operate our Business Continuity Management:
- Emergency Officer
- IT Security Manager
- IT, infrastructure, and operations units
- Services Management with Support

In the case of a crisis, the well-established organization for **emergency processes** can be applied, which has been introduced at AEB several years ago. Organizational aspects on topics such as crisis team, competences and crisis communication have already been regulated there.

3 How is Business Continuity Management organized?

According to the BSI requirements, our emergency concept consists of the following two parts:

An Emergency Planning Concept
It contains all tools that allow us to correctly classify and evaluate our processes according to their relevance to be able to take appropriate emergency measures.
The emergency planning concept deals with both the prevention (reduction of the probability of occurrence or reduction of potential damages) and the emergency response.
The emergency planning concept also provides for regular drills.

An Emergency Manual
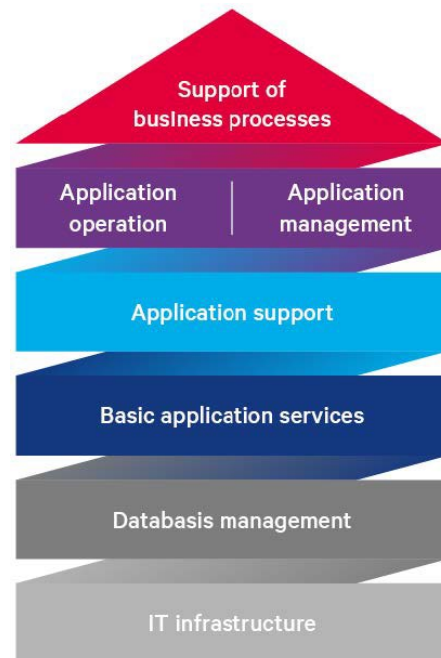It contains specific instructions categorized by service to handle emergencies in an orderly manner.

4 Basic principles of BCM

1. In the case of an emergency, saving life and limb is first and foremost.
2. Restoring our customer's business processes is our utmost concern.
3. The recovery process must be carried out immediately and according to the defined priorities and rules. Our customers' applications take precedence here.
4. If normal operation cannot be resumed directly, emergency operation must be set up at least.
5. For effective prevention and continuous improvements, regular emergency drills must be carried out. Their results are included in the emergency management to secure quality. The same applies to insights from real emergencies.
6. Vigilance, robustness, and thinking in what-if scenarios are important rules.

AEB has visualized all internal structures in a model, also considering the offered services. The AEB application model outlines all the services needed to use, operate, and develop an application. In the considerations and measures concerning the Business Continuity Policy, the recommendations of the German Federal Office for Information Security are taken into account and transferred to the needs of AEB and AEB's customers. AEB matches the methods used for risk analysis and error detection with the recommendations. Therefore, the company's actions are constantly reviewed. To complete AEB's comprehensive security concept, processes are permanently adjusted, expanded and developed further.

Every segment of the AEB application model is subject to multiple security specifications that are implemented as services by AEB or contractual parties after thorough analyses and appropriate preliminary studies.

The following list provides an overview of the measures used. In every area, more detailed instructions, documentation, and tools are available for the employees.

Support of business processes

Application operation | Application management

Application support

Basic application services

Databasis management

IT infrastructure

5 Application-related areas

Support of business processes

In the case of a crisis, we involve our customers to help them keep the negative impacts of the disturbance at a minimum. With an eye on their business process, restoring operations is more urgent than analyzing the cause. This includes offering workarounds in the closest possible collaboration. We believe that making provisions for such workarounds is our task.

Internally and in workshops with our customers, we discuss and develop solutions based on what-if scenarios as additional prevention measures.

Application operation	Application management

With the help of the automated system management and the evaluation of system reports and log files, vulnerabilities can be located before disruptions occur.

By application management we do not only mean automated system monitoring, but our application managers themselves also keep an eye on our applications on a regular basis.

Application support

Errors which occur in a customer system are systematically scheduled and can be examined, detected, and removed via remote system maintenance if necessary. Through a proactive (24/7) monitoring and alerting of the IT, the infrastructure, and all provided services, AEB's Support team is enabled to immediately inform customers about disturbances of AEB services and to initiate further measures.

There is not only a continuous internal exchange within the Support team, but there is also direct contact to the AEB IT specialists of the different areas. This ensures optimal support of AEB customers as well as their active and transparent notification in case of a disruption.

Basic application services

All critical system components have redundant architecture. Due to virtualization technologies and application clusters, it is possible to immediately restore the availability of the systems. AEB uses proven state-of-the-art software and hardware.

All important data is stored multiple times on a Storage Area Network (SAN cross-media storage). If requested and required by the customer, AEB offers different service models tailored to ensure response times, service hours or different priorities of specific services.

Subsequent extensions of services or of the available processing power can be made at any time on request. Bottlenecks can thus be recognized and avoided.

Databasis management

For the AEB database services, there are specifically trained database administrators available. Besides that, we have service agreements with external database specialists in place who are able to maintain and – if necessary – restore the systems and data around the clock depending on the customer's specific needs. A multi-level data backup is made several times a day. Backup copies are regularly placed in separate fire containment sections.

IT infrastructure

The IT infrastructure layer is provided in-house and with the help of other external, carefully selected security service providers for the following related services:

- general power supply and UPS
- fire protection
- air condition and
- physical access control.

The data center is monitored around the clock not only internally, but also externally via a remote connection.

The redundant Internet connection ensures the high availability of the AEB services. The connection to the data center of the German Federal Ministry of Finance for the processing of electronic customs procedures is ensured via a main and backup line. The hardware used meets the latest technical requirements and is maintained by our hardware suppliers as defined in customer service agreements.

Emergency drills based on procedural instructions and processes that are constantly optimized are performed during system maintenance taking place at regular intervals. This helps us ensure that possibly occurring disruptions can be fixed quickly and in an experienced manner.

AEB attaches particular importance to training and continuous education. AEB employees in the IT and service area are specialists who are trained continuously so that that they can fall back on comprehensive know-how.