Business Continuity Management

AEC

Business Continuity Management is one of the important parts of an organisation's strategic and tactical capacity. It concerns a management process that aims to develop effective emergency and recovery plans. These, in tandem with implementing other technical and organisational measures, should ensure the continuity and timely recovery of the organisation's key processes in the event of their disruption or loss due to an accident, natural disaster or security incident.

aec-security.eu

In this area we can offer you:

Full BCM implementation including testing

Business Impact Analysis (BIA), which identifies and analyses user requirements for the resources necessary for their organisation's key processes.

Preparing a continuity strategy - i.e. short and medium term measures to ensure and maintain operations at an optimal level in the event of a disaster.

Methodological support whilst developing Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP), or even comprehensive emergency plans that define the scenarios and procedures needed in the event of specific threats.

Testing the business continuity plans and recovery plans, or full-blown emergency scenarios.

Training those responsible for business continuity or about people's roles in the event of specified emergencies.

In the area of BCM testing we provide:

- Tests for business continuity plans (BCPs),
- Tests for recovery plans (DRP).
- Specific accident scenarios can also be tested.
- Depending on the requirements, it is possible to conduct theoretical tests, practical tests or even tests related to a security incident response (tied in to Red Teaming).

The benefits of BCM

In the event of a disaster or major security incident, BCM will help ensure the organisation's key processes, including ICT operations, are quickly and effectively restored with no negative impact on meeting set business objectives, contractual obligations and customer commitments.

Among the main benefits of implementing BCM services are:

- Reducing the company's losses in the event of an accident,
- protecting the company's good name,
- defining the level of guarantees for customers and partners,
- determining the optimal ratio between investments and the requisite level of availability thanks to:
  - an independent assessment of the availability requirements on the organisation's ICT systems,
  - an identification of the risks and vulnerabilities that pose an immediate threat to the availability of the organisation's key functions and assets.

Our approach

AEC implements BCM based on the experience gained during its long-term work in the ICT security market and in line with recognised standards:

- ISO/IEC 27031, ISO 22313 standards for BCM,
- the ISO/IEC 27000 series of standards focused on information security management

Our methodology can be tailor-made to the requirements of the client or the legislation (e.g. Act No. 181/2014 Coll., on Cyber Security).

Our strengths

Apart from our knowledge of BCM standards, our team also has full technological schooling and experience in continuity management and strategy. This allows us to provide a level of service that far exceeds the standard of conventional providers of documentation for BCM solutions without BCM tests.

Authority

We will provide an organisation with security and continuity support, for instance as a counterbalance to an ICT operations outsourcing supplier.

Determining the BCM process

1

Impact analysis

2

7

Maintenance, testing, updating, training

Business Continuity Management

Risk analysis

3

6

Implementing the measures resulting from the plans

5

4

Creating plans

Developing a recovery strategy

Why have BCM

Why not to have BCM

Protecting your company's reputation.

BCM implementation costs money.

Providing guarantees to customers and shareholders by ensuring continuity.

Someone has to take care of BCM.

Significantly reducing financial losses in the event of a disaster.