Cross-sectional audit of measures taken during system failures in specialist applications

Federal Office for Customs and Border Security, Federal Tax Administration, Federal Office of Information Technology, Systems and Telecommunication

Key facts

Business continuity management (BCM) serves to maintain an organisation's business operations during an incident. This includes preparations for, management of and follow-up after an incident. In spring 2017, a standardised set of federal BCM rules was issued and implemented by the departments and the Federal Chancellery.

Using a maturity evaluation framework, the Swiss Federal Audit Office (SFAO) assessed the status of BCM implementation at the Federal Office for Customs and Border Security (FOCBS) and the Federal Tax Administration (FTA).

As data backup and recovery after an incident are important components of BCM, a second audit was conducted in parallel on the NetBackup security application at the Federal Office of Information Technology, Systems and Telecommunication (FOITT). This evaluated the secure operation and reliability of the backup and recovery processes.

The FOCBS's BCM system has a high degree of maturity

The documentation and concepts for BCM at the FOCBS are very detailed. The critical business processes are identified and the procedure in the event of an incident is described in detail. The planned measures are comprehensible and appropriate for the FOCBS. The IT supporting these processes has redundancy and high availability.

Testing and exercises in relation to BCM measures have been put on hold over the past few years, owing to a number of factors. The planned exercises are described in detail and they should be expanded to cover all areas of the FOCBS over the next few years.

The FTA has made significant progress, but more work is needed

Compared to the previous assessment in 2016, the FTA's BCM has made significant progress. The required documents exist, although some of them are formulated too generically. For example, the critical business processes listed in the business impact analysis are not dealt with consistently during the planning phase.

There is no overarching test concept defining the types of test and stakeholders. However, specific concepts have been drawn up for individual exercises. An evacuation exercise was carried out successfully last year.

Protection against encryption Trojans has top priority

The FOITT systems providing the backup and recovery market supply have redundancy and high availability. The implemented security measures comply with current requirements.

However, the contractually agreed recovery times cannot be completely ensured for large databases, owing to their volume.

Today, encryption Trojans, known as ransomware, pose one of the greatest risks to the availability of systems and databases. Explicit protection against this has not yet been implemented on the backup systems. The FOITT has addressed this, and an external assessment on how to protect data backups against ransomware is planned. This matter should be prioritised, and any measures required should be implemented swiftly.

Original text in German