Security audit of the INFOSTAR database

Federal Office of Justice and IT Service Centre of the Federal Department of Justice and Police

Key facts

Infostar is the centralised register for the electronic registration of civil status events (births, marriages, deaths, etc.), made available to the cantons by the Confederation since 2005. It has almost 1,200 users across 142 civil register offices. The application is managed by the Infostar Unit of the Federal Office of Justice (FOJ) and the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP). A modernisation project costing some CHF 23.7 million is currently under way, with completion originally planned for 2023.

In this audit, the Swiss Federal Audit Office (SFAO) examined whether information security is guaranteed when the application is currently used. It also examined whether the security vulnerabilities in the modernisation project have been remedied and whether the cooperation in the process of handling cyberincidents is working.

The fundamentals of information security are broadly in place for the operation of the current application and the modernisation project, including their integration into the standard infrastructure of the ISC-FDJP. However, there are shortcomings: the application's security documentation and risk analysis need to be updated. The Infostar New Generation project is in a difficult phase: organisational and planning adjustments are required and the testing process needs to be improved. Finally, the foundations of the cyberincident handling process have been laid, but greater operationalisation and better communication are necessary.

Current application: stable performance but outdated security documentation

Through its integration into the standard infrastructure of the ISC-FDJP, the current application benefits from a tried and tested security architecture. User authentication, access rights, encrypted information traffic and redundancies are among the features that have been implemented. Architectural committees monitor the evolution of the system on an ongoing basis.

The application and technical operation activities are described and applied appropriately. User management, malware protection, security backups, monitoring of the infrastructure and periodic testing of its robustness are ensured by specialists. The current solution's performance is stable, but its maintenance is made difficult by the complexity of its programs.

Security governance is in place and roles are defined, staffed, and clearly defined between stakeholders. However, as Infostar's information protection needs have increased, the security documentation is largely out of date. This can lead those responsible to underestimate the risks the solution faces. The security documentation should be updated and a residual risk analysis undertaken and validated.

Modernisation in difficulty, project organisation and testing need improvement

Launched in 2018, the Infostar modernisation project is under way. The work should make it possible to benefit from technical developments and provide answers to the difficulties encountered during maintenance activities. The project is being carried out using agile methodology under the responsibility of the FOJ, which is in charge of defining the business requirements. The ISC-FDJP is in charge of implementation.

The project has been experiencing difficulties for several months, with high staff turnover and the project manager's position being filled on an interim basis. Those in charge are aware of the delicate situation and have defined some immediate measures. A new organisational structure has been put in place and profiles are being sought on the job market. As a result, delays and cost overruns are to be expected. The SFAO decided not to make a recommendation in this regard, but it did ask that the new organisational structure provide for closer integration of the security and operational specialists.

The new application is being implemented within the framework of the standard architecture of the ISC-FDJP. It therefore benefits from the strong security components already in place. The SFAO noted, however, that the project's testing process is not yet fully developed. In particular, the SFAO requested that the depth of the tests, their automation, the non-regression and the handling of defects be rethought.

Cyberincident response and continuity management: integration needs to be improved

The basis for handling cyberincidents is well defined. Roles and responsibilities in this area are actively pursued at the ISC-FDJP. The processes are described, but service users are not sufficiently involved in the implementation of these processes. The Service Centre needs to improve this. It should also reconsider whether it is appropriate to develop response models for different types of incidents. At the time of the audit, the crisis management procedures were being updated, which is why the SFAO refrained from issuing a recommendation.

Incident management and reporting systems are in place, as are contact points and reporting channels. Actions and decisions taken during an incident are documented. Monitoring instruments are in place, and events are logged and can be analysed using tools.

Business continuity management procedures are defined within each administrative unit, but the SFAO found that there is a risk that they are not sufficiently integrated. It has advised the FOJ to organise continuity management exercises for Infostar that include users and service providers. The aim is to improve coordination between the parties involved and to identify any weaknesses in the process.

Original text in French