AUDIT

Audit of application releases in an agile environment

Federal Office of Information Technology, Systems and Telecommunication

KEY POINTS

The Federal Office of Information Technology, Systems and Telecommunication (FOITT) recently upgraded its Atlantica private cloud IT infrastructure. In particular, it implemented a new software container management platform. This technology enables an application's code to be grouped together with the configuration files and components needed to run it. The work, carried out as part of the Amboss programme, was completed by the end of December 2023 at a cost of some CHF 13.2 million. It also involved the creation of new process chains and tools for the automated release of applications known as CNCICD pipelines. These pipelines are of particular importance in terms of the internal control system (ICS). They must ensure that tests to check compliance with the requirements placed on an application solution have been successfully completed before it goes into production mode.

In this audit, the Swiss Federal Audit Office (SFAO) examined whether the FOITT's specifications and processes ensure that requirements – particularly non-functional requirements such as security, architectural conformity, incorporation of ICS needs, etc. – are met in all application releases. The SFAO found that an initial version of the CNCICD pipelines is operational and already in use. However, only some of the non-functional requirements are covered by automatic tests in the releases. The other requirement categories can be tested through manual validation steps. Several issues are still pending, and the FOITT is working on them. The SFAO also recommended that the ICS perspective be strengthened in this work.

A first version of the pipelines is in place, but the coverage of requirements through automatic tests is limited

A structured approach was used to implement the CNCICD pipelines. The specifications stipulated that the possibilities offered by cloud environments had to be exploited to the full, while ensuring security. This work resulted in a complex combination of tools and processes, covering the stages of application development and deployment of solutions in continuous mode. The pipelines guide developers and operators through the version management of code objects and the testing and validation (integration) activities. They then support them in preparing software packages and distributing them to production infrastructures (deployment). Various ancillary functions, such as event logging and the storage of sensitive information, are also made available. Although some issues are still pending, this first version has proved its worth: four application solutions have already been released through the pipelines, and more than a hundred are currently being worked on. The adoption process is progressing, and the FOITT and service recipients are acquiring experience. Adjustments remain possible.

Applications can only be released through a pipeline. In order to facilitate the adoption of this principle by internal and external developers, the FOITT has created a wealth of documentation in the form of descriptions, guides, standards, videos and checklists. A specific type of pipeline has been implemented for containerised applications delivered on a turnkey basis by external suppliers. This means that these applications also have to pass the tests defined in the tool chains before they can be deployed on the target production infrastructure. This ensures that both internal and external developers can make appropriate use of the CNCICD pipelines and ensure that the defined requirements are met.

The automatic tests incorporated in the CNCICD pipelines only cover requirements relating to basic IT protection. These tests, which are not all mandatory, focus on looking for vulnerabilities, apparent identifiers in program lines and the quality of application code. However, for other types of requirements, whether functional or not, automatic tests were not used. In these cases, lengthy definitions specific to each application would be necessary.

Instead, the FOITT favoured the possibility of defining manual validation steps or incorporating a test loop into an ad hoc tool. In order to encourage service recipients to accept the system, a middle way between automation and the incorporation of manual steps was therefore chosen. However, this still leaves a large share of the responsibility for the correct implementation of the requirements to the development teams.

The SFAO believes that this first version of the CNCICD pipelines offers a reasonable starting point in terms of incorporating requirements control. It assumes that the FOITT will continue to keep pace with technological developments in testing tools and push for automation wherever possible.

Options exist for temporarily bypassing tests

Since automatic tests sometimes return false-positive results or are not always relevant to a given environment, an option to deactivate them ("whitelisting") was introduced. According to the defined process, this exception must be duly documented and validated by the beneficiary and the service provider. The exception is valid for a limited period of time. For the SFAO, this controlled deviation from the obligation to test applications is acceptable.

Other ways of getting around it exist. Firstly, developers can copy an existing pipeline and modify the copy to remove the mandatory test steps. They can then theoretically use it to release applications without testing them. Mechanisms for protecting pipeline definitions by means of cryptographic signature were included in the Amboss programme. However, it has not yet been possible to implement them, due to the lack of a compatible product on the market. Pipeline protection is therefore inadequate for the time being, but the FOITT is keeping this shortcoming on its list of pending issues. Secondly, it is still possible to detect such cases a posteriori by analysing pipeline execution logs. For these reasons, the SFAO decided not to issue a recommendation on this point.

The SFAO stated that it had not been able to assess the effectiveness of the controls implemented for CNCICD pipelines. The FOITT was able to show that the relevant data is available, but it has not yet been formally analysed for a representative sample of releases.

Operationalisation is under way, but the ICS perspective needs to be better integrated

A committee is in charge of steering the CNCICD platform, defining its governance and the priorities for its future development. Representatives of the FOITT's Business Solutions and Platform Services domains, as well as security specialists, sit on this committee. However, the ICS perspective is not explicitly represented on the committee.

A reference framework describing the main pipeline-related functions is in the process of being adopted. Among these functions, higher-level activities are already being conducted. These include monitoring operations and checking the security and fitness of pipelines and applications. A pipeline security audit was carried out at the end of December 2023. However, the processes and responsibilities stemming from the functions described in the terms of reference have not yet all been defined and institutionalised, but the committee is working on their operationalisation. The SFAO has therefore decided not to make a recommendation on this point. However, it has recommended that the ICS perspective be strengthened within the committee and its work agenda.

Original text in French