Management of the Artemis System

Background

In order to continuously respond to calls, and in line with fire departments in several large Canadian cities, the Centre de communication en sécurité incendie (CCSI) of the Service de sécurité incendie de Montréal (SIM) has been using a computerized call-dispatch system named Artemis since November 2007. The SIM, which operates 67 stations, is the only fire department of its kind in the entire agglomeration of Montréal, ensuring the safety of Montréal's population.

To effectively fight fires and respond to calls, it is crucial that the SIM, specifically the CCSI, be able to rely on a highly efficient system with high availability to dispatch incoming calls among the service's 2,739 staff members. In 2022, they responded to 118,916 calls for fire emergencies or as first responders throughout the Ville de Montréal (the City).

Purpose of the audit

To determine whether the existing control mechanisms ensure the sound management and high availability of the SIM's Artemis system.

Results

Overall, we conclude that the City has several control mechanisms in place to ensure the sound management of the Artemis system. Indeed, the definition of the roles and responsibilities, the process used to manage patches and updates, the monitoring of service levels, the specialized human resources, the high-privilege accounts and the IT succession plan are adequate.

However, some areas require improvement, including the Artemis system's authentication parameters, the procedure used to manage high-privilege logical access, the functional documentation of the Artemis system's environment as well as the automated incident alert mechanisms.

Main Findings

Governance

- The stakeholders' roles and responsibilities with respect to the governance and management of the Artemis system are documented.

Logical Access Management

- There are no obsolete high-privilege accounts in the Artemis system.
- The City's logical access management standard, which outlines the requirements pertaining to the authentication parameters, is not applied to version 2.6 of Artemis.
- There is no procedure for managing high-privilege logical access to Artemis, Smartemis and Artemis Web.

Patch and Update Management

- The new version of Artemis was implemented in accordance with best practices. However, this process is not documented in any given procedure.

Incident Management

- The process for managing incidents in Artemis is based on good practices.
- There are no automated alert mechanisms in place in the Artemis environment. However, CCSI staff is present at all times and would therefore be able to detect any problems in real time.

Monitoring

- Service levels with the integrating supplier are defined and monitored during steering committee meetings.

Specialized Resources

- The SIM and the Service des technologies de l'information (STI) have sufficient specialized human resources to maintain the Artemis system in operational condition.

Functional Documentation

- Artemis's functional documentation is not systematically updated every time changes are made to the system's environment.

System Continuity

- An adequate system continuity plan has been developed and is tested annually.

In addition to these results, we made various recommendations to the business units, which are presented in the following pages.