Management of the Artemis System

Service de sécurité incendie de Montréal
Service des technologies de l'information

3.7.

March 1st, 2023

2022 Annual Report
Auditor General of
the Ville de Montréal

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.

List of Acronyms

Artemis
Artemis system

CAC
Comité d’approbation des changements

CAD
Computer-assisted dispatch

CCSI
Centre de communication en sécurité incendie

CDS
Centre de service TI

City
Ville de Montréal

DSP
Division Sécurité publique

GPRAO
Artemis troubleshooting solution

MOP
Manuel d’organisation de projet

RACI
Responsible, Accountable, Consulted and Informed

RFC
Request for change

RMS
Response management system

SIM
Service de sécurité incendie de Montréal

SSDO
Système de suivi des données opérationnelles

STI
Service des technologies de l’information

Table of Contents

1. Background

The 9-1-1 service officially began operations in Montréal on December 1, 1985. With the advent of mobile phones, this service has evolved and is today able to receive all calls from landline phones and smartphones. The Centre de communication en sécurité incendie (CCSI) of the Service de sécurité incendie de Montréal (SIM) was dispatching calls and having to deal with a significant increase in the number of calls. In 2002, following the municipal mergers, the SIM decided to replace its obsolete dispatch system.

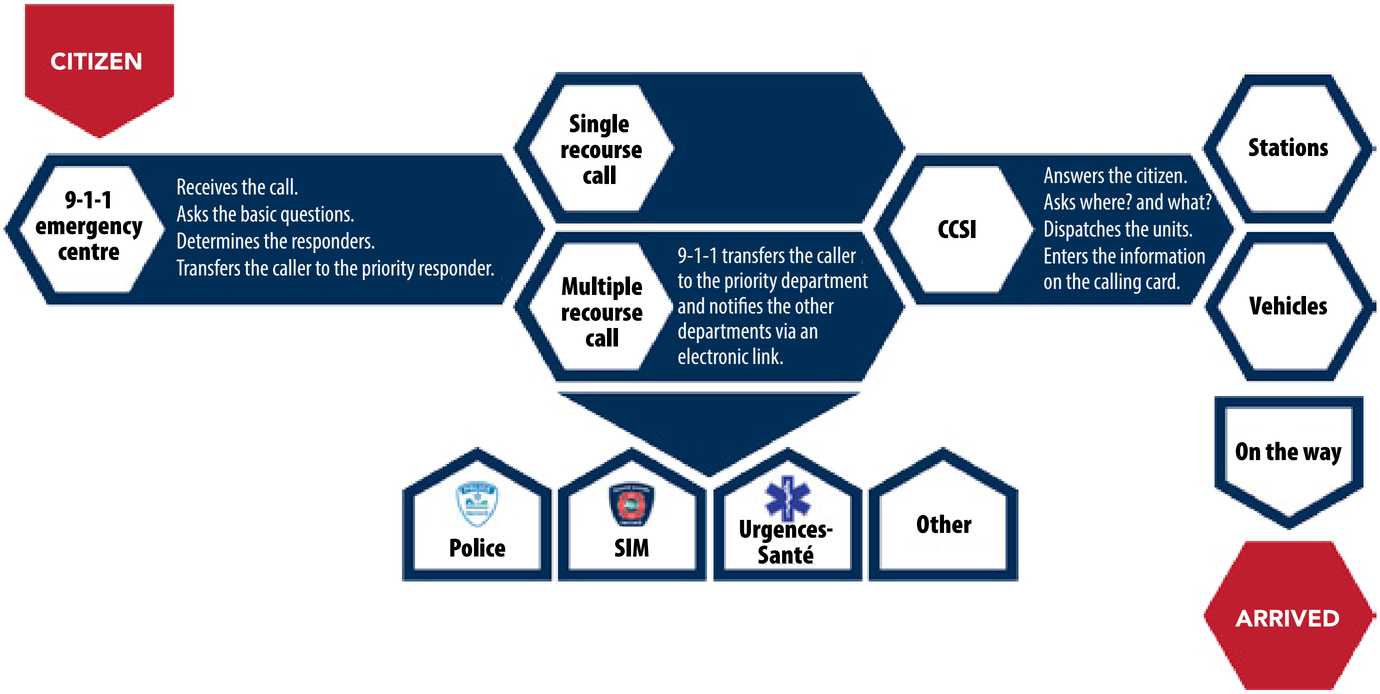
Like the fire departments of several major Canadian cities, the SIM has been using a computerized call dispatch system — i.e., a Computer-assisted dispatch (CAD) system — commonly known as Artemis, since November 2007. That same year, the SIM began providing prehospital emergency care as a first responder to 911 emergency calls.[1] The SIM, which operates 67 stations, is the only fire department of its kind in the entire agglomeration of Montréal, ensuring the safety of Montrealers.

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).

[1] "SIM – 2021 Annual Activity Report," page 21 (available in French only).

1.1. Description of the Artemis System

Here is a diagram of the 911 calls and calls to the CCSI's Artemis CAD system:


CITIZEN
9-1-1 emergency centre
Receives the call.
Asks the basic questions.
Determines the responders.
Transfers the caller to the priority responder.
Single recourse call
Multiple recourse call
9-1-1 transfers the caller to the priority department and notifies the other departments via an electronic link.
Police
SIM
Urgences-Santé
Other
CCSI
Answers the citizen.
Asks where? and what?
Dispatches the units.
Enters the information on the calling card.
Stations
Vehicles
On the way
ARRIVED

Source : Presentation of the CCSI division titled "Module 1 – Présentation du CCSI aux recrues."

Artemis is the SIM's CAD system, historically published by a solutions provider. The system handles calls received from emergency centres. It allows the CCSI's agents to coordinate responses in the field and to dispatch resources throughout the island of Montréal. Every second counts when the SIM is called as a responder, and the Artemis system reduces delays and optimizes operations.

The Artemis system is composed of several connected applications so that the SIM's responders can manage emergencies from start to finish:

- **Version 2.6 of Artemis (Artemis 2.6)**: This system is the main module that the CCSI uses through the dispatch centre's computers, in both the main and backup centres. It communicates with the Artemis mobile and Artemis station modules as well as with Smartemis and Artemis Web.

  Its functionalities include taking and processing calls, managing responses and vehicles, relocating,[2] reassigning vehicles, managing Artemis maps mapping and sending comments or instructions.

[2] Relocating: consists of redistributing vehicles according to the calls received to ensure optimal coverage of the territory.

- **Artemis maps**: The CSSI uses Artemis's mapping component to plan, supervise responses and give firefighters in vehicles and fire stations a detailed view of the sector of intervention.

- **Artemis mobile**: This Artemis module is installed on the computers on board emergency trucks. It communicates with Artemis 2.6 and provides map-based information to determine, among other things, the best route based on street closures. It allows firefighters to record their status regarding the call underway in real time. In addition, it presents key information related to the response site, such as the presence of hazardous materials and the state of the construction.

- **Artemis station**: This Artemis module is installed on the computers of the stations' control centres, each connected to a printer, for receiving and acknowledging the mission orders for response requests. It provides the information the firefighters need to respond to a call. This information is used to determine the resources required (number and type of trucks, number of firefighters, etc.).

- **Smartemis**: This application has four functions:

  1. Notifications: receives real-time intervention notifications as soon as they are dispatched;
  2. Intervention overview: provides a detailed view of the interventions;
  3. Vehicle overview: provides a real-time view of the vehicles and their status;
  4. Navigation: shows how to get to the intervention sites.

  Both the SIM's managers and the firefighters use Smartemis according to their access profile.

- **Artemis Web**: This application provides access to Artemis's operational data outside of dedicated user stations (the CCSI, the backup centre and the stations) and to certain functions (e.g., intervention overview, vehicle overview, response histories and response timelines) from a web browser. It is accessible to all SIM personnel, with restrictions according to their logical access profile.

- **Artemis troubleshooting solution (GPRAO)**: This is the Artemis solution installed on a stand-alone workstation (laptop). It operates in disconnected/local mode in the event of a CCSI network failure.

- **Système de suivi des données opérationnelles (SSDO)**: This system captures and compiles operational data from the SIM's interventions. The database (DB) contains the data from Artemis that is automatically transcribed into the SSDO's fields. It is a mechanism for reconciling data from the CAD system, actions undertaken and facts recorded at the scene of the response. For approval purposes, the SIM's managers sign off on the interventions using this DB's interface.

  The system's main functions are to identify the causes of fires, to enter data on the actions undertaken, to record facts at the scene of the response and to produce reports for the Ministry of Public Security.

At the City level, the Artemis system is managed by two of the City's business units and two vendors:

- The SIM:
  - The SIM's Centre de services – planification stratégique et opérationnelle provides support for managing logical access to Smartemis and Artemis Web during the transfer to the Division de la planification opérationnelle of the CCSI;
  - The Centre de services – intervention, composed namely of the SIM's CCSI, provides support to users and communicates their business needs to the STI's Division Sécurité publique (DSP);
- The STI:
  - The Division solutions d'affaires – systèmes corporatifs of the DSP of the Direction Sécurité publique et justice of the Service des technologies de l'information (STI) is responsible for the technology infrastructure side and provides operational support as well as support for projects to evolve the Artemis environment. It works closely with the integrating supplier, responsible for the outsourcing of the Artemis environment;
- The integrating supplier is responsible for the maintenance – operation and evolution – of the Artemis environment. It works with the Artemis solution provider;
- The Artemis solution provider (solution provider) has developed the Artemis solution and is ultimately responsible for evolving the system as required by the SIM.

2. Purpose and Scope of the Audit and Evaluation Criteria

2.1. Purpose of the Audit

Pursuant to the provisions of the *Cities and Towns Act* (CTA), we performed a performance audit on the SIM's management of the Artemis system. We carried out this mission in accordance with the *Canadian Standard on Assurance Engagements* (CSAE) 3001 of the CPA Canada Handbook – Assurance.

The purpose of this audit was to determine whether the control mechanisms implemented to manage the Artemis system ensure the sound management and high availability of the SIM's Artemis system.

2.2. Evaluation Criteria

Our assessment is based on criteria we deemed valid under the circumstances, namely:

1. Governance

The roles and responsibilities involved with system governance and management are documented, complete, approved, up to date, formally distributed to and implemented by stakeholders.

2. Logical Access Management

Guidance on authentication parameters is defined and applied appropriately to Artemis.

A procedure for managing logical access (creating, modifying, revoking, revising, removing and monitoring privileged access rights) has been developed, and the stakeholders that manage access know and follow the procedure in place.

3. Patch and Update Management

A formal patch and update management process has been defined and is being applied appropriately.

Formal and regular follow-up is carried out with all of the stakeholders involved in the management of patches and updates, and the appropriate actions are applied.

4. Incident Management

An incident management procedure has been developed, approved, distributed to and implemented by stakeholders. The procedure is reviewed at a predetermined frequency.

5. Monitoring

Adequate monitoring is performed by the supplier, including service level definition and reporting, as well as logging predefined security events and tracking them on a regular basis.

6. Specialized Resources

There is a sufficient number of dedicated dispatch resources spread out throughout the Artemis management community.

There is both a human resources succession plan and an Artemis training program.

7. Functional Documentation

Technical documentation covering the configuration, use and environment has been developed by the stakeholders involved in the management of these systems (i.e., the STI, the SIM and the integrating supplier).

The existence of these documents is known, they are up to date and have been approved and they are used by all of the stakeholders concerned.

8. System Continuity

A system continuity plan is in place and is tested annually. If necessary, action plans are developed and implemented based on the test results.

The responsibility of the Auditor General of the City is to provide a conclusion regarding the purpose of the audit. To that end, we gathered sufficient and appropriate evidence on which to base our conclusion and obtain a reasonable level of assurance.

The City's Auditor General applies the Canadian Standard on *Quality Management 1, Quality Management for Firms that Perform Audits or Review of Financial Statements, or Other Assurance or Related Services Engagements*. This standard requires the City's Auditor General to design, implement and operate a quality management system that includes policies and procedures to ensure compliance with ethical rules, professional standards and applicable legal and regulatory requirements. In the performance of her work, the City's Auditor General also complies with the rules regarding independence as well as with the other ethical rules of Québec's *Code of ethics of chartered professional accountants*, which are based on the principles of integrity, professional competence and due diligence, confidentiality and professional conduct.

Our audit work covered the period from October 2021 to December 2022. Our work consisted of conducting interviews with employees, reviewing various documents and conducting surveys that we deemed appropriate to gather the necessary evidence. However, we also took into account information that was sent to us up to March 1st, 2023.

At the end of our work, a draft audit report was presented for discussion to the relevant managers in the audited business unit. The final report was then forwarded to the management of the business units concerned as well as to the City's Direction générale.

2.3. Scope of the Audit

Our audit work focused on the Artemis environment, including:

- Artemis 2.6;
- Artemis Maps;
- Artemis mobile;
- Artemis station;
- Smartemis;
- Artemis Web;
- Artemis troubleshooting solution (GPRAO);
- Système de suivi des données opérationnelles (SSDO).

3. Audit Results

3.1. Governance

Sound governance of the Artemis system consists foremost of determining the roles and responsibilities of the various stakeholders involved in managing the system. This is formalized in a RACI (Responsible, Accountable, Consulted and Informed) responsibility matrix.

The stakeholders that govern and manage Artemis are the STI, the SIM and the integrating supplier in collaboration with the solution provider.

We found that the governance and management of Artemis have been based on a project governance model – Système de gestion des interventions (SGI), exploitation et évolution – since its first draft dating back to 2007. The model therefore consists primarily of a contract monitoring committee that meets as needed, depending on the issues and problems at hand. There is also the SGI's steering committee, which meets every two weeks. This committee tracks incidents and issues, as well as the progress of requests for change, and reports on the various actions assigned to the stakeholders sitting on either committee.

We noted that roles and responsibilities are defined in the following documents:

- The *Manuel d'organisation de projet* (MOP), in the Rôles et responsabilités and Gouvernance sections, as well as in *Annexe A (Tableau des responsabilités contractuelles).* This is the stakeholders' ultimate reference;
- The Artemis 2.4 operation file also lists the roles and responsibilities in the responsibility table, by component;
- The integrating supplier is responsible for the daily operation and evolution activities of the SGI, commonly referred to as maintenance. There is a binding contractual agreement to this effect;
- The RACI on the Artemis 2.4 upgrade and modernization project is dated October 31, 2016, and lists the roles and responsibilities at each stage of the project.

These documents are not up to date, as Artemis 2.6 rather than 2.4 is the version currently in use. However, this is a recent version change (September 2022) and the changes are only minor. Transfers of responsibilities to the STI — e.g., level 1 support[3] — are not reflected, nor are the organizational changes. A request to have the MOP revised has been initiated with the integrating supplier for this purpose.

We consider the items listed above to form a matrix of responsibilities for Artemis, particularly in the context of a project that is outsourced to the integrating supplier with the collaboration of the solution provider. No recommendation is required since the functional documentation is in progress.

[3] Level 1 support concerns the IT service centre that answers users' calls and directs them to the appropriate internal or external teams.

3.2. Logical Access Management

Logical access management has two components: authentication parameters and the procedure for managing logical access to the IT systems.

3.2.1. Authentication Parameters

The authentication parameters provide a formal login (user code and password) framework to connect to the IT systems. This required defining an authentication framework and applying it to the IT systems appropriately. These authentication parameters concern the use of user codes and a password strategy (i.e., the minimum length, complexity, password validity period and history, as well as the number of failed attempts, duration of account lockout and other parameters).

We noted the following:

Artemis 2.6 and Its Artemis Maps Submenu

Artemis users with write access in Artemis can only log in from their workstations located in the premises of the CCSI and under the supervision of a supervisor.

Authentication to Artemis 2.6, and to its Artemis maps submenu, consists of logins whose user account formats vary according to function. The CCSI's team uses personal accounts that can be reassigned after employee departures.

The SIM uses an external file to control the use of these accounts, which are associated with users' personnel numbers. The functionalities of the authentication method implemented in Artemis 2.6 — length, complexity and password history — do not comply with the City's access management frameworks (*the Directive sur la gestion des accès logiques and the Standard sur la gestion des accès logiques*, dated July 2020 and January 2021, respectively).

Improper configuration of authentication parameters could allow ill-intentioned individuals to gain unauthorized access to Artemis and its components.

RECOMMENDATION 3.2.1.A.

We recommend that the Division Sécurité publique of the Direction Sécurité publique et justice of the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, analyze options to increase the robustness of the Artemis 2.6 authentication parameters in accordance with the Standard sur la gestion des accès logiques.

Artemis Mobile and Artemis Station

No human authentication is required to access Artemis mobile and Artemis station. Their authentication to Artemis 2.6 is performed automatically through a script (using the IP address and the physical location of the device—workstation or vehicular computer—in a station or vehicle). These systems do not grant privileged access. They are used to provide firefighters with real-time information on interventions in order to respond efficiently to calls received from citizens. They must be active 24 hours a day, 7 days a week.

No recommendation is necessary.

Smartemis and Artemis Web

Authentication to the Smartemis mobile application, from the same solution provider as Artemis, is performed only when the app is installed on a smartphone. The user is required to provide the personnel number, U code and telephone number. Once Smartemis has been installed, it no longer requires the user to enter authentication information. Exceptionally, the six managers can add another device to Smartemis.

Authentication to Artemis Web is done using the U code, in the case of managers, and the employee's personnel number, for operational teams and firefighters, as well as the Artemis 2.6 password. Following discussions among stakeholders, the option to install a directory for Artemis Web in the extranet[4] was not deployed.

Users of Smartemis and Artemis Web (accessible only through the City's intranet) access information from Artemis 2.6. No transactions or information updates are allowed or possible. Both systems use the Artemis 2.6 authentication parameters. The password is normally the personnel number. The SIM gives priority to high availability and easy access.

In our opinion, the Smartemis and Artemis Web authentication parameters are adequate. No recommendation is necessary.

GPRAO (Artemis Troubleshooting Solution)

GPRAO is an Artemis troubleshooting solution that is accessible in multi-user mode as well as on a stand-alone workstation. The multi-user version is used when the Artemis servers are down. This solution does not offer the possibility to communicate with the stations. As of November 2022, upon return to normal status (i.e., at the end of an outage), the GPRAO's data is automatically synchronized with the SSDO.

The GPRAO, in both multi-user and stand-alone modes, requires neither a user account nor a password. The multi-user mode requires the entry of the extension number.

The GPRAO stand-alone station is located in a secure room to which only the CCSI's personnel has access.

No recommendation is necessary.

[4] The extranet is a private network controlled between partners whereas an organization's intranet is accessible only to its employees.

Système de suivi des données opérationnelles (SSDO)

Created in 2001, the SSDO is a reporting application that captures all of the data associated with an intervention and organizes it in the form of a searchable log. Two report formats are associated with a response: one consulted by the dispatchers and one to be completed by the firefighters. Every 10 seconds, the SSDO receives interventions from Artemis.

The SSDO can only be accessed from one of the City's internal workstations or through the VPN,[5] from the SIM's intranet. Authentication to the SSDO's database is by password — as per the City's password policy — combined with the U code in the case of managers, and the employee's personnel number in the case of operational crews and firefighters.

None of the authentication parameters — password length, complexity and history — in this password policy are consistent with the City's Standard sur la gestion des accès logiques. However, to ensure compliance, the SIM could request that the parameters be changed. No modifications have been made to facilitate access for the firefighters.

Non-robust authentication parameters could result in unauthorized resources being able to access reports.

RECOMMENDATION 3.2.1.B.

We recommend that the Division Sécurité publique of the Direction Sécurité publique et justice of the Service des technologies de l'information and the Service de sécurité incendie de Montréal analyze the relevance of increasing the robustness of the Système de suivi des données opérationnelles authentication parameters.

3.2.2. Procedure for Managing High-Privilege Logical Access

A logical access management procedure details the process for creating, modifying, revoking, reviewing, and deleting accounts as well as for monitoring logical access rights, particularly in the case of privileged access. High-privilege access is granted to system administrators and authorized resources who require more extensive access to data to perform their tasks.

This procedure should cover, among other aspects:

- Limited and restricted use of privileged access to authorized resources;
- Formal approval of all requests to use an account with privileged access;
- Deletion of unused user accounts suspended for a certain period of time;
- Regular review of the access rights associated with the accounts;
- Monitoring high-privilege accounts.

We found that the January 2021 Standard sur la gestion des accès logiques has specific requirements for high-privilege accounts. These requirements should be detailed in a logical access management procedure that provides the steps to follow to create, modify, revoke, review and delete accounts as well as to monitor logical access rights for this type of account.

[5] The VPN is a virtual private network that makes it possible to link two remote computers through a single private connection, or tunnel, using a larger network infrastructure, such as the web or a wide area network (WAN). Once activated, a VPN acts as a direct connection to a private network.

We noted the following:

Artemis 2.6 and Its Artemis Maps Submenu

No procedures for managing privileged logical access to Artemis have been developed, approved and disseminated to the stakeholders in accordance with the January 2021 Standard sur la gestion des accès logiques.

Only the creation of users and the association of users with profiles are described in the solution provider's administrator training document.

Two separate entities have privileged access, namely the integrating supplier responsible for Artemis support and maintenance and certain members of the SIM's personnel. Since the spring of 2021, at the request of the head manager of the Division Centre de communication d'urgence, the integrating supplier processes and closes all logical access requests.

However, there are logical access management processes in place to create and modify privileged access. Contrary to the general rule, user accounts are deactivated and access rights remain associated with the accounts once users have left. Consequently, access rights are not revoked and accounts are not deleted. In addition, there is no review or monitoring of access rights.

Until the former manager left in April 2022, high-privilege logical access requests were processed directly in the system. We did not find any documentary evidence to this effect. A creation form was implemented in November 2022 by the integrating supplier during our work.

In the absence of requests to create, modify or revoke privileged logical access to the Artemis system, no effectiveness testing was conducted for the period from October 2021 to September 2022. However, we found no trace of obsolete accounts in the Artemis 2.6 privileged user lists.

The lack of a procedure for managing high-privilege logical access could result in the mismanagement of high privilege logical access and unauthorized access being granted to Artemis 2.6 and its data.

RECOMMENDATION 3.2.2.A.

We recommend that the Division Sécurité publique of the Direction Sécurité publique et justice of the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, develop, approve and disseminate a privileged logical access management procedure applicable to the Artemis 2.6 system.

Artemis Mobile and Artemis Station

When a fire station and vehicle are integrated into Artemis 2.6, the computers are configured with scripts to establish an automatic connection with the integrating supplier. Thus, no privileged logical access management applies to Artemis mobile and Artemis station.

No recommendation is necessary.

Smartemis and Artemis Web

The integrating supplier processes and closes requests for logical access management to Smartemis and Artemis Web from the SIM. Privileged access is only granted to six of the SIM's resources, the integrating supplier and the Artemis 2.6 solution provider.

No procedures for managing privileged logical access to Smartemis and Artemis Web have been developed, approved and disseminated to the stakeholders in accordance with the January 2021 Standard sur la gestion des accès logiques.

However, the processes applied overall are adequate. A Google form is used to approve requests to access Smartemis on a personal phone.

In the absence of requests to create, modify or revoke privileged access to Smartemis and Artemis Web, no effectiveness testing was conducted for the period from October 2021 to September 2022. However, we found no trace of obsolete accounts in either of these systems' privileged user lists.

The lack of a procedure for managing high-privilege logical access could result in the mismanagement of high-privilege logical access and unauthorized access to Artemis 2.6 data being granted through the Smartemis and Artemis Web systems.

RECOMMENDATION 3.2.2.B.

We recommend that the Division Sécurité publique of the Direction Sécurité publique et justice of the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, develop, approve and disseminate a privileged logical access management procedure applicable to Smartemis and Artemis Web.

GPRAO (Multi-User and Stand-Alone Mode)

This application does not require a user account or password and works only with system administrator accounts. Thus, no privileged logical access management applies to it.

No recommendation is necessary.

SSDO (Système de suivi des données opérationnelles)

The processes for creating, modifying and revoking access rights involve the use of the IT service management tool to open and close a request for access the SSDO. No formal procedures for managing logical access have been developed by the DSP team of the Direction Sécurité publique et justice of the STI that is responsible for the SSDO. However, in addition to the eight SSDO specialists of the STI, two of the SIM's managers have privileged access rights (access to all SSDO screens and reports).

This division uses a pilot application to manage the logical access. A team of five people processes these SSDO access requests for the SIM. The creation and modification processes are adequate. However, in the event of an employee departure, the SIM does not create a request to revoke access rights and the account therefore remains active.

A single request to create privileged access to the SSDO was made for the period from October 2021 to September 2022, in accordance with sound practices. There were no requests to change or revoke privileged access to the SSDO during this period. We found no trace of obsolete accounts in this system's privileged user lists.

Given the small number of users, the impacts of not having a procedure for managing privileged logical access to the SSDO are minimal. No recommendation is therefore required.

3.3. Patch and Update Management

Upgrading a CAD system such as Artemis is complex, as the system must always be available. Changes that would have significant impacts on the SIM's operations should therefore be avoided. For this type of service, every second counts. It is crucial that Artemis be kept as stable as possible.

The integrating supplier, in collaboration with the solution provider, is responsible for evolving Artemis according to the City's needs.

We found that the relevant stakeholders know and use the patch and update management process that has been in place for several years now.

We were informed of the following elements of this process:

- It covers patches and updates following an incident, an anomaly on Artemis or a Request for change (RFC). The integrating supplier assumes responsibility and works with the solution provider to develop a patch by following its certification process. Testing takes place on the supplier's side in the laboratory environment, with its test grid, and the SIM performs operational testing in its training environment before approving the final implementation. Otherwise, the failures raised by the SIM are forwarded to the integrating supplier, who sends them back to the solution provider until the SIM grants its final approval;
- Planning the deployment of a patch takes into account whether the operation is urgent or not. The STI, after having received the SIM's test grid, drafts a documented acceptance report for approval by the SGI's steering committee and a time slot is determined. The STI completes the form of the Comité d'approbation des changements (CAC) with the documentation required by the CAC. The STI presents the type of intervention, its impact and the rollback procedure to the CAC. Once the authorization is obtained, it informs the SIM by email. The deployment date is determined by the CAC in accordance with the authorized change schedule to ensure that Artemis's critical teams are available. The planned deployment is communicated to the affected teams within the STI as well as to the heads of the SIM's sections;
- While updates and patches are being deployed, the necessary actions are taken to ensure that production is not affected during the process. The integrating supplier then communicates with the SIM. The stakeholders verify that the Artemis system is functioning properly, as problems not related to the patches could occur. If such problems are found, the STI documents them for correction by the integrating supplier;
- All of the patches and updates are discussed and the steering committee follows up on them at its bi-weekly meetings.

We found that this Artemis patch and update management process was followed and fully implemented during the implementation of the Artemis 2.6 system. It included two patches, one evolution and no RFC. In addition, this process follows good documentation, impact assessment, prioritization and authorization, monitoring, quality control and closure practices.

While all of this is in place, it is not written down in a formal Artemis patch and update management procedure. Each step is documented in an appropriate deliverable.

The absence of an Artemis patch and update management procedure could result in deviations in applying the steps for this critical system.

RECOMMENDATION 3.3.A.

We recommend that the Division Sécurité publique of the Direction Sécurité publique et justice of the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, develop, approve and disseminate a patch and update management procedure.

3.4. Incident Management

An incident is an unplanned event that can cause the interruption or degradation of a service. Sound incident management therefore aims to restore service as quickly as possible in accordance with contractually defined service levels.

We noted that the Artemis incident management process consists of documentation developed by the STI, in collaboration with the SIM, and by the integrating supplier. The documents are accessible to all of these stakeholders and consist of the following:

- "Arbre de décision – Système de gestion des interventions (SGI) et Artemis (SIM) V02.2": This document is used to transfer the incident to the most appropriate team;
- "Documents de connaissance sur le SGI et Artemis": These describe how to create an incident and how the Artemis support provided by the Centre de service TI (CDS) functions with the integrating supplier as well as the support groups.

The incident management procedures that apply to Artemis can be found in the IT service management tool.

We were informed that the integrating supplier remains primarily responsible for managing incidents. After the CDS has entered the incidents, it processes all incidents and closes them in the IT service management tool. As such, the supplier's incident management procedure is governed by the contractual agreement that binds it to the City.

At the bi-weekly meeting of the SGI's steering committee, SGI stakeholders (i.e., at a minimum, the integrating supplier's project manager, a resource from the STI, an operational resource of the SIM and a CCSI resource, with additional participants as needed) track incidents, including major incidents and problems experienced by users.

From the incident list obtained from the STI, we randomly selected 14 incidents out of the 135 critical-, high-, and moderate-priority[6] incidents and one incident out of the 11 low-priority incidents that occurred during the period from October 1, 2021, to September 30, 2022. This list included only one critical-priority incident and 127 high-priority incidents. Our sample of incidents is detailed as follows:

- 1 critical-priority incident;
- 12 high-priority incidents;
- 1 moderate-priority incident;
- 1 low-priority incident.

In applying the incident management procedure, we made the following findings:

There is no automated alert mechanism in place for reporting an incident caused by an application problem in the Artemis environment. However, since CCSI personnel is present 24 hours a day, 7 days a week, 365 days a year, these problems would be detected in real time.

The flow of an incident alert is as follows: a call is made by the CCSI to the CDS, which transfers it to the integrating supplier for support. All incidents require this supplier's intervention. A team of 7 people from the CDS is dedicated to supporting the SIM.

The CDS's incident management process follows sound practices for documentation, classification and prioritization, categorization through to incident resolution and closure. Any call from headquarters to the CDS is always considered urgent. A major incident escalation process has been implemented for Artemis. The CDS team dedicated to the SIM and the head of major incidents take charge of the incident. This practice is designed to coordinate the work with the required stakeholders. Otherwise, the SIM communicates directly with the STI to keep managers informed of the outage and its progress.

Since the integrating supplier does not have automated alert mechanisms to detect an outage in real time, it initially relies on the SIM's calls.

The lack of automated alert mechanisms in Artemis could increase the time needed to respond to a critical incident.

RECOMMENDATION 3.4.A.

We recommend that the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, analyze the relevance of implementing automated real-time alerts to signal Artemis system failures.

[6] The incident's priority is determined by its impact and its urgency. Priority will determine the relative importance of incidents and resources will be allocated accordingly.

3.5. Monitoring

Active monitoring is done using a tool that allows the user to see in real time the activities or transactions taking place on a computer system. Security event logging (i.e., passive monitoring) aims to keep track on an ongoing basis of who is doing what in a computer system. This applies especially for users whose accounts have elevated privileges (referred to as "super users").

We found that the MOP defines service levels for operating and evolving Artemis. The following service level is always under the supplier's responsibility:

- CAD availability rate (Artemis) = (time of period - downtime - maintenance time) / time of period. This criterion for measuring the quality of the supplier's maintenance services must reach the threshold of 99.5%. (According to the information obtained for 2022, no failures occurred.) Otherwise, an analysis will be triggered to find the cause and define the required corrective actions.

The service provider monitors the application component for which it is responsible. It uses a tool to monitor the Artemis servers and databases and verify the connection status. No automated alerts were deployed on its end.

The provider also has an operational monitoring tool for Artemis interfaces (GPRAO, SSDO, fire hydrants). The STI uses monitoring tools for the infrastructure underlying Artemis to verify that the servers and network are in good condition.

The SIM also has an operational monitoring tool it uses to synchronize the GPRAO. In addition, because the service is available 24 hours a day, 7 days a week, 365 days a year, the CCSI's team detects, in real time, any outages or performance problems affecting Artemis.

We noted that both service level monitoring and the announcement of any future intervention by the STI that may have an impact on the Artemis environment are carried out during steering committee meetings. This is coordinated with the resources of the STI, the SIM and the service provider.

Accountability

We found that the provider creates dashboards as agreed upon, based on the service levels defined in the service agreement. As a result of the City assuming responsibility for the single window, the infrastructure and the network on behalf of the SGI, the SIM has requested a redesign of the SGI's dashboard. This dashboard has been revised to focus solely on the time-in-service service level, the downtime and the percentage of SGI availability including the Artemis environment.

We were informed that the dashboard was not routinely sent to STI and SIM recipients each month in 2022. The list of recipients is under review. The STI made ad hoc requests to analyze the relevance of the metrics, the maintenance time and the failures before the monthly dashboard was reintroduced. In addition, at steering committee meetings, all parties involved in the management of incidents review the current month's dashboard presenting a summary of the year to date.

Given these items, no recommendation is necessary.

3.6. Specialized Resources

Artemis comes from a solution provider that specializes in computerized dispatch systems. There is a distinct integrating supplier responsible for the evolution and operation of the Artemis environment as per the binding service agreement with the City. It is primarily the integrating supplier that has all the in-depth knowledge of this environment. During a major change, or even a minor change, the integrating supplier works with the Artemis solution provider as well as with the STI and the SIM.

We noted the following:

Service des technologies de l'information (STI)

Within the Division solutions d'affaires – systèmes corporatifs of the DSP, no one is specialized in the Artemis system. The integrating supplier is the expert in this field and provides the City with the services of a dedicated team. However, this division of the STI supports the supplier in managing this environment and operates in a collaboration and task prioritization perspective.

No resource is available at all times to answer the SIM's calls. The goal is to support the SIM by serving as an interface with the integrating supplier. The 13 resources making up this team — 3 who are directly related to Artemis and 11 who are available on an as-needed basis — as well as the 11 resources supporting other STI teams (e.g., a project manager, an administrator, an IT analyst, an operations manager) represent a sufficient number of specialized resources to support operations and projects concerning the Artemis environment.

No recommendation is necessary.

Service de sécurité incendie de Montréal

The SIM's CCSI comprises approximately 60 resources, three of which have administrator access to Artemis and play a liaison role between the CCSI, the integrating supplier and the STI's DSP. The members of this team, composed mainly of agents (i.e., dispatchers and radio operators), a senior attendant responsible for tracking the types of trucks and responses, as well as supervisory managers and a division manager, are Artemis end users for the most part.

The SIM was the object of a reorganization in August 2022. Based on this reorganization, the SIM needs to review the composition of its teams, including the actual needs for resources to support the use of Artemis. Artemis training is primarily derived from the supplier's documentation as well as from internal documents developed for the agents.

We consider that there is an adequate number of specialized support resources.
No recommendation is necessary.

3.7. Functional Documentation

The Artemis environment is composed of several interrelated components and modules. Up-to-date functional documentation ensures the support, operation and evolution of the environment as well as the transfer of knowledge to the specialized resources.

The technical documentation was developed primarily by the Artemis solution provider and the City's integrating supplier. The latter handles all technical changes that relate to Artemis and is responsible for documenting them. The SIM, for its part, developed training documents for its agents that are accessible in Artemis. Since 2017, the integrating supplier has been responsible for configuring Artemis.

We found that other documents were developed and approved with the collaboration of all stakeholders, including:

- Artemis 2.4 run book dated August 26, 2020: This document addresses the Artemis 2.4 emergency response dispatch systems upgrade and modernization project. It defines the project's operating methods and aims to support the maintenance of activities as well as to define routine operations that are to be carried out on the system. In addition, it contains a technical description and several diagrams, including a network diagram of the Artemis environment, and a data flow diagram of Artemis 2.4 applications without Smartemis and Artemis Web. These have been in production since October 2020;
- MOP, dated February 10, 2020: This document is considered the ultimate reference for all the stakeholders. It covers the project organization for the SGI's operation and evolution, of which the Artemis environment is an integral part. This version of the document should be updated annually to reflect the various changes agreed upon between the service provider and the City. This one covers the November 14, 2018, release of version 2.4 of Artemis, Artemis Maps and a new virtual server architecture.

All of this existing documentation concerns version 2.4 of Artemis. Since then, this system was upgraded to version 2.5 on October 8, 2020, and, most recently, to version 2.6, on September 7, 2022.

We were informed that a process was initiated with the service provider in September 2022 to perform the annual MOP review, following the implementation of Artemis 2.6. The Artemis 2.4 run book is a more complex document to update.

The incompleteness and outdatedness of the Artemis system documents could affect the process of adding functionalities, the root cause analysis of problems and the quality of the service provided.

RECOMMENDATION 3.7.A.

We recommend that the Service des technologies de l'information and the Service de sécurité incendie de Montréal, with the collaboration of the integrating supplier, review and update the technical documents, including the MOP (*Manuel d'organisation de projet*) and the Artemis system's run book

3.8. System Continuity

To operate Artemis, there are procedures that need to be mastered and various methods that are designed to ensure that the service is available at all times. The system continuity plan exists to ensure this availability. It is therefore essential to have a complete and up-to-date system continuity plan (a continuity environment that replicates the production environment) and to perform annual continuity tests. These help to raise any issues and address them with action plans, improve performance and update the continuity environment.

System Continuity Plan

We found that a system continuity plan had been developed. It covers the Artemis environment and all of the components of the SIM's SGI. This was achieved with the collaboration of all the stakeholders involved in this continuity plan, i.e. the integrating supplier, the various teams of the STI and the SIM. The objective is to document the recovery of the SIM's SGI following an outage due to a major incident.

We noted in the MOP that the supplier is responsible for providing documentation for Artemis environment continuity procedures for which it is responsible. In the event of a disaster, to ensure SGI continuity, the supplier's support team then executes these planned and documented continuity procedures.

We were informed that the SIM's "Plan de relève Service de Répartition" is being reviewed and updated to reflect the changes made to the telephone system in October 2022. More changes are expected to the fire station system in 2023. The implementation of Artemis 2.6 on September 7, 2022, constitutes minor changes that have no impact on the system continuity plan. We noted that it includes all the information on the IT and telecommunications portions expected from such a plan. In addition, this plan is updated annually and whenever there is a significant change in the IT environment's components. It is subject to the approval of the relevant STI and SIM directors. It is distributed through an internal platform that is accessible only to the authorized resources of the various internal teams of the STI, the SIM and the supplier.

We were informed that, regardless of the type of major incident affecting the IT component of the SIM's SGI, the switchover to the secondary site requires the involvement of the integrating supplier's team to activate the Artemis system. For redundant infrastructure, the switchover is automatic.

Artemis System Continuity Environment

We found that a system continuity environment was deployed for the Artemis system in two data processing rooms located in two separate remote sites. There are redundant telecommunications with two separate public operators. Finally, active redundancy is integrated into the computerized emergency call management system (telephone consoles), enabling the CCSI to handle emergency and administrative calls.

Continuity Plan Testing

We noted that the continuity plan is tested annually and is also used during planned major changes. A post-mortem is produced when issues or problems arise, and action plans are defined to rectify the situation. No issues were raised during the last annual test conducted in 2021.

We believe that the system continuity plan is adequate. No recommendation is necessary.

4. Conclusion

Overall, we conclude that the Ville de Montréal (the City) has control mechanisms in place to ensure the sound management of the Artemis system.

Indeed:

- The stakeholders' roles and responsibilities with respect to the governance and management of Artemis are documented;
- The process applied during the implementation of the new version of Artemis has, at every step, complied with sound patch and update management practices;
- The service levels provided by the integrating supplier are monitored by the steering committee;
- There is a sufficient number of specialized human resources to support Artemis;
- There are no obsolete high-privilege accounts in Artemis or its components;
- An adequate system continuity plan for the Artemis environment is tested on a regular basis.

However, some areas need improvement:

- The Artemis 2.6 authentication parameters do not meet the City's logical access management standard. However, write access to Artemis is only allowed from a workstation installed on the premises of the Centre de communication en sécurité incendie (CCSI) of the Service de sécurité incendie de Montréal (SIM) and under the supervision of a supervisor;
- The procedure for managing high-privilege logical access in Artemis 2.6, Smartemis and Artemis Web is not documented;
- Artemis's procedure for managing patches and updates in production is not documented;
- The functional documentation of the Artemis environment is not systematically updated each time a change is made. Nevertheless, there are few differences between Artemis 2.6, implemented in September 2022, and the previous version (2.5);
- There is no automated alert mechanism in place for reporting an incident in the Artemis environment. However, CCSI staff is present at all times and would therefore be able to detect any production problems in real time.

More specifically, here are the details according to the following evaluation criteria:

Governance

The roles and responsibilities of the stakeholders involved in the governance and management of Artemis are documented, including in the *Manuel d'organisation de projet* (MOP) and the Artemis 2.4 run book. Also, a RACI (Responsible, Accountable, Consulted and Informed) matrix on the Artemis 2.4 upgrade and modernization project was defined in October 2016. These documents are not up to date, as Artemis 2.6 is the version that has been in production since September 2022. However, a review has been requested to this effect and is underway.

Logical Access Management

The City's January 2021 logical access management standard outlines the requirements pertaining to authentication parameters and follows sound practices. However, these parameters are not applied in Artemis 2.6 or in the Système de suivi des données opérationnelles (SSDO).

Procedures for managing privileged logical access to Artemis, Smartemis and Artemis Web have not been developed, approved and disseminated to the stakeholders, which could lead to cases of unauthorized access. However, overall, the informal privileged logical access management processes in place are adequate for Smartemis and Artemis Web. Processes used to create and modify privileged access to Artemis are also adequate.

Evaluation Criterion – Patch and Update Management

An Artemis patch and update management process was defined and applied appropriately when Artemis 2.6 was implemented. In addition, this process follows good documentation, impact assessment, prioritization and authorization, monitoring, quality control and closure practices. However, this process is not found in an Artemis patch and update management procedure. The lack of this procedure could lead to deviations in applying the steps to be followed for this critical system.

Evaluation Criterion – Incident Management

An Artemis incident management procedure has been developed, approved and disseminated to stakeholders. In addition, the incident management process follows sound practices for documentation, classification and prioritization, and categorization through to incident resolution and closure. Since the integrating supplier does not have automated alert mechanisms to detect an outage in real time, it relies on the calls from CCSI personnel, who are present at all times. The lack of automated alert mechanisms in Artemis could increase the time needed to respond to a critical incident.

Evaluation Criterion – Monitoring

With respect to operation and evolution, service levels with the integrating supplier and service provider are defined in the MOP. This supplier performs the monitoring for the application side. Service levels are monitored during steering committee meetings. Effective reporting the stakeholders is done.

Evaluation Criterion – Specialized Resources

In addition to the integrating supplier, all of the internal stakeholders involved in managing Artemis have sufficient dedicated resources to support the operations and projects within the Artemis environment and to support the use of the system.

Evaluation Criterion – Functional Documentation

The existing documentation developed and approved by all of the stakeholders involved in Artemis management is not reviewed or kept up to date. It covers an earlier version of Artemis that presents few differences with version 2.6 currently in production. The incomplete and outdated Artemis functional documentation could affect the root cause analysis of problems.

Evaluation Criterion – System Continuity

An adequate system continuity plan has been developed. It covers the Artemis environment and all the components of the SIM's SGI (Système de gestion des interventions). The continuity plan is tested annually.