3.3.

Centralized Identity and Access Management

Service des technologies de l'information

February 8, 2022

2021 ANNUAL REPORT

Auditor General of the Ville de Montréal

Centralized Identity and Access Management

Background

Centralized Identity and Access Management (IAM) is defined as all processes and technological tools used in the centralized management of users and their access rights to information systems and applications. IAM provides all users, internal and external, appropriate access in a timely manner, while reducing the number of identifiers and passwords that need to be remembered. IAM control mechanisms are adapted to the security and sensitivity levels of the information being accessed. To achieve this, organizations adopt standards and industry best practices. They enable the implementation of standardized policies and control mechanisms that ensure the protection of data.

In 2016, the Ville de Montréal (the City) has launched two projects to meet the IAM needs of citizens and employees, they're known as GIA Citoyens and GIA Employés, respectively. The GIA Citoyens project is currently under the responsibility of the Division solutions numériques of the Service des technologies de l'information (STI), while the GIA Employés project comes under the responsibility of the STI's Direction sécurité de l'information. Because of the departure of key employees and changes in their duties and responsibilities, the GIA Employés project is being relaunched.

In the meantime, the GIA Employés serves about 30,200 employee accounts, 1,700 external user accounts, 560 application accounts and integrates 125 applications. As for the GIA Citoyens, it serves more than 255,000 citizen accounts and integrates 70 applications.

Purpose of the Audit

To determine whether the IAM process and its control mechanisms implemented by the City provide assurance that they do not present any major risk to the confidentiality, integrity and availability of data.

Results

In the case of GIA Citoyens, we can conclude that the process and control mechanisms put in place do not present any major risk to the confidentiality, integrity and availability of data. However, we believe that ongoing work to adopt the Pan-Canadian Trust Framework (PCTF) for digital identities must continue. Note that the Trust Framework defines and standardizes processes and specifies privacy requirements, which would optimize the security of data and services available to citizens.

For GIA Employés, given that the project is being relaunched, our findings do not allow us to conclude that this IAM provides adequate risk management for data confidentiality, integrity and availability. We identified gaps in the areas of governance, definition of roles and responsibilities, project strategy, as well as in risk analysis and process documentation. Moreover, the technological tools currently in use will be replaced. Therefore, there is no IAM process yet. Rather, the controls in place respond to decentralized administrative mechanisms.

Main Findings

Governance

GIA Citoyens:

- The IAM strategy is properly documented;
- The process owner is not formally identified and the roles and responsibilities are not fully documented;
- The risk analysis is not completed;
- Assurance levels, which establish security requirements based on the confidentiality level of the information to be accessed, are not formally established.

GIA Employés:

- The process owner is not formally identified and the roles and responsibilities are not properly defined. Moreover, management frameworks are not finalized;
- The GIA Employés project has shortcomings regarding the active involvement of the Comité de sécurité de l'information (CSI) and business units, the inclusion of all types of users, the analysis of the current context (processes and technologies), the documentation of business requirements, the standardization of phases and deliverables, as well as the absence of the target architecture;
- The risk analysis and proposed controls do not meet the requirements of an IAM;
- The assurance levels, which establish security requirements in accordance with the confidentiality level of the information being accessed, are not yet formally established.

User Management (Identities)

- Citizen identity management is adequate apart from the lack of an account deletion mechanism.

Authentication Management

- The GIA Employés and GIA Citoyens authentication are not adapted to the different confidentiality levels of the information being accessed.

Access Management

- Citizen access management meets the least-privilege and need-to-know criteria;
- The process for periodic review of citizens' access is not in place.

Integration of Applications into IAM

- This process is adequate in GIA Citoyens. However, teams must ensure that the applications integrated into GIA Citoyens are also integrated into the Dossier citoyen intégré (DCI) and that any exceptions are formally justified.

In addition to these results, we formulated various recommendations to the business units, which are presented in the following pages. The business units concerned were given the opportunity to agree to these recommendations.

List of Acronyms

CISO	Chief Information Security Officer
CSI	Comité de sécurité de l'information
DCI	Dossier citoyen intégré
DIACC	Digital ID & Authentication Council of Canada
GIA	Gestion centralisée des identités et des accès *(french translation of IAM)*
IAM	Centralized Identity and Access Management
RASCI	Responsible, Accountable, Support, Consulted and Informed
SRH	Service des ressources humaines
STI	Service des technologies de l'information

Table of Contents

1. Background

Large-scale organizations such as the Ville de Montréal (the City) have extensive information resources that serve many trades and administrative functions. Users often require many passwords to access those resources. This can lead to a downgrade in security, since users tend to neglect security instructions by reusing the same passwords from one application to another.

Protecting access to information resources is even more important nowadays because of the increased number of people working remotely. Users' computers do not fall within the traditional limits of the organization's network. An environment that is insufficiently secured could be the target of cybercriminals, and a compromised identifier is often the entry point for more serious attacks, such as mass data theft and ransomware.

In order to render its IT environment more secure, an organization must implement Centralized Identity and Access Management (IAM). IAM is defined as all processes and technological tools used in the centralized management of users and their access rights to information systems and applications. IAM provides all users, internal and external, appropriate access in a timely manner. IAM control mechanisms are adapted to the security and sensitivity levels of the information being accessed. To achieve this, organizations adopt standards and industry best practices, which include standardized policies and control mechanisms to protect identities and access to data.

The organizational benefits of IAM include:

- Improved user experience by reducing the number of identifiers and passwords to remember when accessing information assets;
- Less administrative overload related to account management thanks to self-serve technological tools and automated processes for authorizing, approving, modifying and revoking access rights;
- Optimized security for accounts and information assets through the implementation of multi-factor authentication and the application of risk-based policies;
- Standardization of access profiles in compliance with best practices, such as the principles of least privilege and need-to-know and the segregation of incompatible duties;
- Simplified mechanisms available to information asset owners for periodic access reviews;
- Warning and monitoring mechanisms capable of detecting and dealing with unauthorized accesses.

1.1. Overview of Centralized Identity and Access Management at the Ville de Montréal

For the purpose of standardizing applicable requirements to access to non-public information under its responsibility, the City issued a directive and a standard pertaining to logical access management. These management frameworks are applicable to all employees as well as individuals from outside firms and partners having access to the City's information. The directive defines the responsibilities of the main stakeholders, including the Comité de sécurité de l'information (CSI) and the Chief Information Security Officer (CISO). The CSI oversees the adoption of a cross-sector approach to logical access management that is common to all business units but adapted to the business context of each. This should ensure adequate risk management. The CISO's responsibilities include delivering and administering identifiers, as well as implementing security measures to mitigate the risks related to logical access.

In terms of solutions currently in place, the City initiated two projects to meet the IAM needs of employees and citizens. This led to the implementation of two distinct solutions, one for citizens and the other for employees. GIA Citoyens, known as the "*identité numérique des citoyens*" was an initiative arising out of the "Présence numérique – Fondation" project. It began in 2016 under the responsibility of the "Bureau de l'expérience citoyenne". When that unit was disbanded, the Division solutions numériques of the Service des technologies de l'information (STI) assumed management responsibility. The GIA Employés project, on the other hand, is under the responsibility of the STI's Direction sécurité de l'information. That initiative also began in 2016 as part of the IT security and continuity program. However, due to the departure of key employees and changes in responsibility, the project is being relaunched.

The approach adopted by the "*identité numérique des citoyens*" project was focused on citizens and on improving the services offered. For this project, the City implemented a portal where citizens could create an account and receive services online. GIA Citoyens currently serves more than 255,000 citizen accounts and integrates 70 applications.

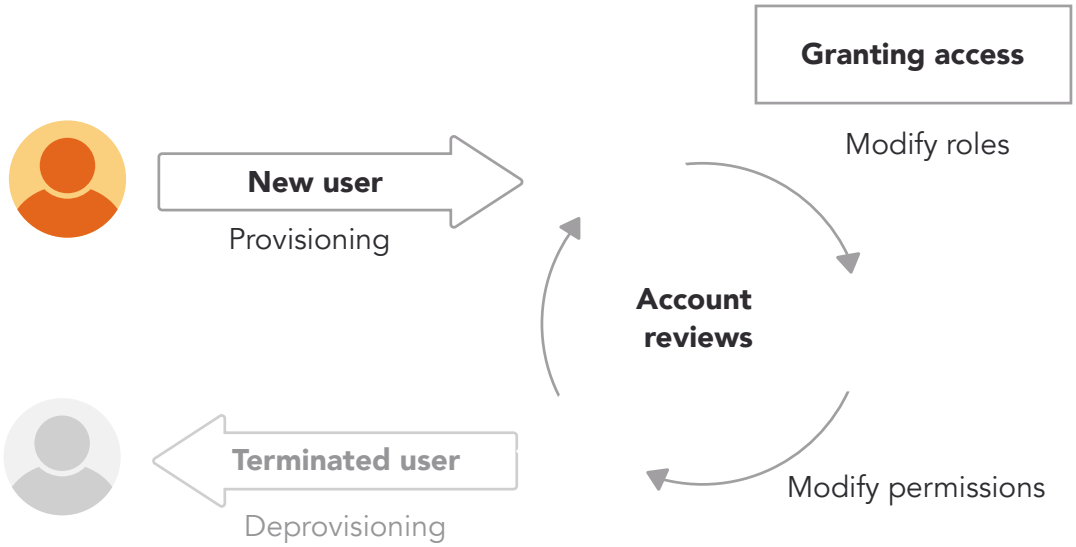
The GIA Employés project adopted a more technological approach. The team has prioritized improved access and authentication. Due to technological and financial issues, however, the tools selected for the project need to be replaced. In the meantime, the tools in place currently serve more than 30,200 employee accounts, about 1,700 external user accounts and nearly 560 accounts for the 125 integrated applications. IAM processes are currently based in decentralized administrative procedures under the responsibility of each business unit. Work pertaining to business needs, processes and the selection of standards to adopt should resume in 2022. Moreover, interim solutions will be deployed.

1.2. Account Life Cycle

In this section, we provide a theoretical description of the various components in the life cycle of a user account:

FIGURE 1

Account Life Cycle

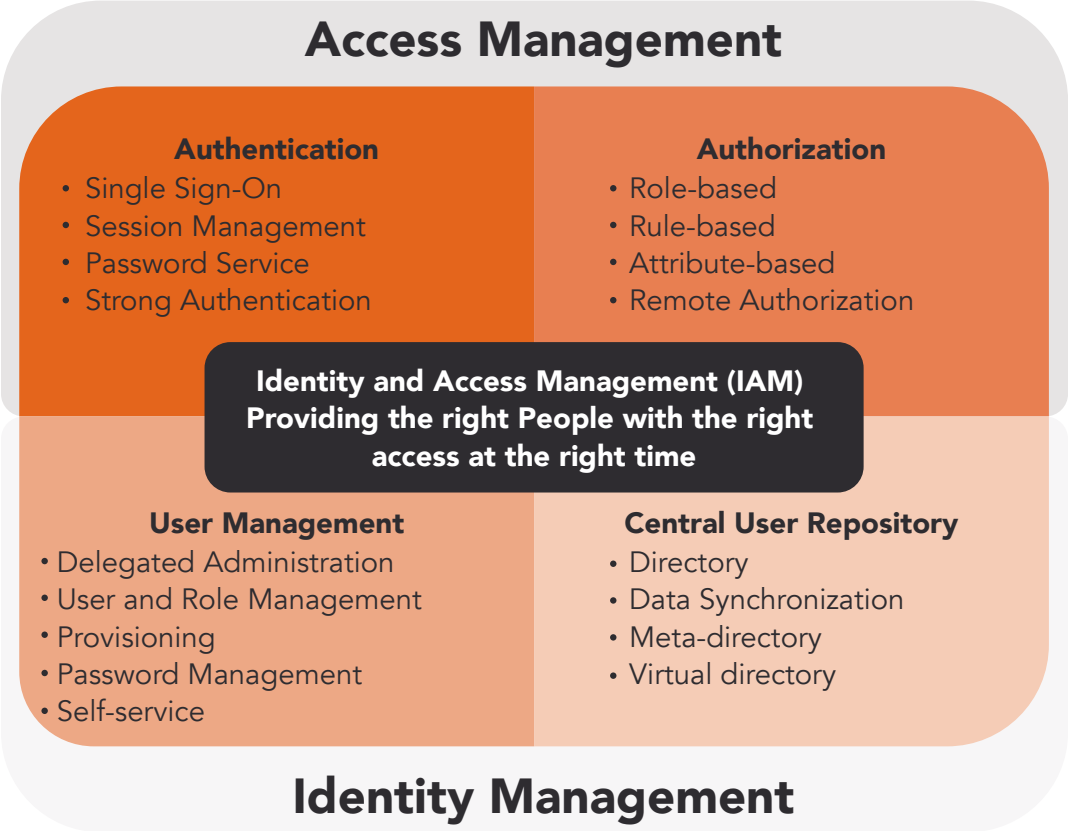


- *Provisioning:* An account is created when a new user arrives. The identity of the new user is verified to ensure that it meets the security requirements of the assets being accessed. For example, an email address is sufficient to register for an informative website. However, access to a highly confidential asset may require, for instance, a criminal record check;
- *Granting access:* Once the account has been created, authorization is granted to access the necessary assets. Granting access is always the result of an automated or manual approval process. Assigning roles is a simplified way of granting access rights. For example, assigning the role of accountant defines access to the appropriate finance systems and is automatically granted to accountants when they are hired;
- *Modify access:* When access needs modification because the user has assumed a new job, role or duties, or when assets are added or withdrawn, the user's access privileges need to be updated. Modifying access requires prior approval;
- *Account reviews:* Access is reviewed periodically by the asset owners to ensure that there are no unauthorized users. Access is monitored continually to ensure proper use and to detect any incidents;
- *Deprovisioning:* When a user leaves or no longer requires their account, access owners request that the account be closed, which results in its deactivation. Deactivated accounts are destroyed in accordance with each organization's information preservation standards.

The entire life cycle of accounts just described can be implemented simply and securely using IAM. To achieve this, processes and technological tools are put in place to cover the following four areas (see Figure 2):

FIGURE 2

Framework for Centralized Identity and Access Management



- ***Identity Management***:
  - ***User management***: Used to manage the accounts and roles of identities from provisioning to deactivation and destruction. This includes user provisioning, password management, granting and maintaining profiles, as well as setting up self-serve tools. These simplify identity management through features such as self-managed profiles and the automatic reset of multifactor authentication mechanisms and passwords;
  - ***Central user repository***: It presents an aggregated view of an organization's identities. The central directory provides identity information to other departments and is used to verify identification information submitted by clients. By acting as a single infrastructure that centralizes all accounts and user rights for every application, the central directory simplifies operations and facilitates access for users;

- ***Access Management***:
  - ***Authentication***: Management feature that allows a user to provide sufficient identification information to obtain initial access to a specific system or resource. Authentication can be achieved by using one or more authentication factors such as passwords, access tokens, text messages and so forth. Once a user has been authenticated, a session is created and referenced throughout the interaction between the user and the system. A session is locked when the user disconnects or when other events are triggered (e.g., user inactivity timeout);
  - ***Authorization***: Feature used to determine whether a user is authorized to access a particular resource. Generally speaking, authorization is managed in accordance with predetermined roles. IAM also provides mechanisms that simplify the periodic review of access, detect authorization conflicts and automatically withdraw access rights when an employee leaves, changes role, is suspended, etc.

2. Purpose and Scope of the Audit

Pursuant to the provisions of the *Cities and Towns Act*, we conducted a performance audit of the IAM system. We carried out this mission in accordance with the *Canadian Standard on Assurance Engagement* (CSAE) 3001 of the *CPA Canada Handbook – Assurance*.

The purpose of this audit was to evaluate the IAM process and control mechanisms in place at the City in order to ensure that they present no major risk to the confidentiality, integrity and availability of data.

The role of the Auditor General of the Ville de Montréal is to provide a conclusion regarding the purpose of the audit. To that end, we gathered sufficient and appropriate relevant evidence on which to base our conclusion and obtain a reasonable level of assurance. Our assessment is based on criteria we deemed valid for the purposes of this audit. These criteria are presented in Appendix 5.1.

The Auditor General of the Ville de Montréal applies the *Canadian Standard on Quality Control* (CSQC) 1 of the *CPA Canada Handbook – Assurance* and, accordingly, maintains a comprehensive quality control system that includes documented policies and procedures with respect to compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. The Auditor General also complies with the independence and other ethical requirements of the *Code of ethics of chartered professional accountants*, which are based on the fundamental principles of integrity, professional competence and due diligence, confidentiality and professional conduct.

Our audit covered the period from April to November 2021. It comprised holding employee interviews, examining various documents and conducting surveys that we deemed appropriate in order to obtain the necessary evidentiary information. We took into account information that was sent to us up until February 8, 2022.

Upon completing our audit, we submitted a draft audit report to the managers concerned in each audited business unit for discussion purposes and to obtain action plans and timelines for implementing the recommendations.

3. Audit Results

3.1. Governance

3.1.1. Roles, Responsibilities and the Process Owner

Sound governance of IAM consists in defining the roles and responsibilities of the various stakeholders for each management-related task. This is formalized in a RASCI (Responsible, Accountable, Support, Consulted and Informed) responsibility matrix.

It is also important, for a process of this scale, to define the person responsible for it, thereby establishing clear accountability for every action that requires a chain of validation. The process owner is responsible for operational management. That person must be involved in every major change and every application migration.

GIA Employés

In the audited documents, we found several RASCI responsibility matrices for the management of specific IAM tools.

Only the RASCI responsibility matrix for the single sign-on tool and for two-factor authentication[1] has been formally approved.

Our content review of the other RASCI responsibility matrices revealed the following deficiencies:

- There is no RASCI responsibility matrix covering IAM as a whole;
- For the most part, defined tasks pertain to technological tools;
- For most tasks, the person accountable is not indicated;
- The roles and responsibilities of the other stakeholders are not specified (e.g., the Service des ressources humaines (SRH), users, application developers and other administrative units).

The City's access management directive identifies the following responsibilities:

- The CSI for the adoption of a cross-sector approach to access management;
- The CISO for identity management and security.

[1] Two-factor authentication: Authentication requiring the user to provide two credentials belonging to two distinct authentication factors, e.g., a password and a token installed on a telephone. (Source: Office québécois de la langue française)

Despite what is stipulated in the directive, we found that there was some confusion in the responsibilities related to IAM. When we met the security team, we were informed, among other things, that:

- Identity management is the responsibility of the SRH;
- Access management for consultants is the responsibility of the STI's Bureau de projets;
- The Centre de services TI is responsible for the access service requests it processes;
- Each business unit is responsible for managing its own access to applications.

On the other hand, during our meetings with the SRH, the Bureau de projets and the Centre de services, we learned that while they do have a role to play, those units do not consider the above-mentioned areas to be under their responsibility.

We conclude that the roles and responsibilities set out in the directive were not properly communicated. In addition, there is a deficiency in the definition, documentation and approval of roles and responsibilities for the IAM process overall.

The lack of a formal definition of an owner, as well as deficiencies in the definition of roles and responsibilities pertaining to IAM, could result in operational shortcomings such as:

- Failure to take responsibility for decisions pertaining to IAM;
- Ineffective collaboration among teams (e.g., users being redirected to the wrong teams for access or incident management);
- Granting access to applications without prior validation;
- Unperformed tasks, omissions and uneven actions taken with respect to IAM.

3.1.1.A. Recommendation

We recommend that the Direction sécurité de l'information of the Service des technologies de l'information formally define the owner of the Centralized Identity and Access Management process.

3.1.1.B. Recommendation

We recommend that the Direction sécurité de l'information of the Service des technologies de l'information communicate the roles and responsibilities of the access management directive to the various stakeholders.

3.1.1.C. Recommendation

We recommend that the Direction sécurité de l'information of the Service des technologies de l'information document, approve and diffuse the roles and responsibilities pertaining to Centralized Identity and Access Management as a whole.

GIA Citoyens

During our audit tests, we found that:

- The roles and responsibilities are well known to the main stakeholders. This was confirmed during interviews and in documents collected pertaining to the processes and technological tools in place;
- A RASCI responsibility matrix has been defined and covers development, support, changes in technology and citizen communications;
- The various stakeholders have been identified;
- The owner of GIA Citoyens has not been formally identified;
- The RASCI responsibility matrix has not been formally approved;
- Certain functions have not yet been documented and accountability has not been assigned.

The failure to formally identify an owner, as well as deficiencies in the RASCI responsibility matrix documentation, could lead to operational shortcomings such as:

- Failure to assume responsibility for decisions pertaining to IAM;
- Unperformed tasks, omissions and uneven actions taken with respect to IAM.

3.1.1.D. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information officially identify the owner of GIA Citoyens.

3.1.1.E. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information complete, approve and distribute roles and responsibilities for GIA Citoyens.

3.1.2. Management Frameworks for Centralized Identity and Access Management

The publication of policies and directives provides a management framework for certain processes, thereby limiting the risk of inconsistency in the actions taken and preventing access procedures from being bypassed and privileges abused. Typically, IAM should set out basic principles to clarify the following:

- Centralized identity management: from provisioning to deactivation or deprovisioning;
- Centralized access management: for the authentication and management of access rights to information assets (granting, modification, monitoring, withdrawal and periodic review).

GIA Employés

The directive and standard for logical access management are published on the City's intranet. It should be noted that these management frameworks concern access management as a whole and target all identities and assets managed by the City. These documents are up to date, complete and formally approved. In addition, the directive has been sent to all employees.

As for more specific management frameworks pertaining to the life cycle of IAM accounts, we examined the following processes:

- Processes and procedures for the arrival, suspension and departure of an employee;
- Granting and withdrawal of privileged accounts;
- Access management for consultants;
- Guiding principles for the management of contracts that specify certain tasks pertaining to access management;
- Compendium of guides and instructions related to IAM drawn from the Centre de services TI knowledge base used by their agents.

We noted that the processes and procedure listed above do not correspond to IAM.

We also found a lack of procedures for the following:

- Access management specifically for GIA Employés in compliance with the management frameworks;
- Periodic access reviews;
- Life-cycle management of third-party accounts (suppliers, partners, consultants, volunteers and other similar categories);
- Life-cycle management of accounts related to hardware assets (such as servers, printers and workstations) and software (including databases, software applications and websites).

Given that the IAM project is ongoing, processes and procedures pertaining to IAM have not yet been documented.

A lack of IAM processes and procedures could lead to the risk of non-uniform IAM practices, as well as to non-compliance with the roles and responsibilities of stakeholders in terms of access to the City's information assets. This could result in unauthorized access to sensitive information.

3.1.2.A. Recommendation

We recommend that the Direction sécurité de l'information of the Service des technologies de l'information document the processes and procedures specific to Centralized Identity and Access Management and ensure that they are distributed to the stakeholders.

GIA Citoyens

Citizen identities are managed using the Dossier citoyen intégré (DCI) platform, which has two web interfaces:

- Mon Compte pour les citoyens;
- Mon Compte – vue employés, which employees use to process the online requests of citizens.

- ***Citizens Web Interface***

A privacy policy and account terms of use are accessible on the City's portal. The policy is also accessible when a citizen account is created or a password changed. We identified the following procedures on the citizen portal:

- Account provisioning;
- Citizen and business account modification;
- Account deletion at the request of the citizen.

These documents are up to date, complete, formally approved and duly published.

On the other hand, we found that:

- No procedure is in place for the periodic review of accounts;
- The procedure triggered by a request to delete a citizen account is manual and undocumented.

- ***Employees Web Interface***

Employees can use "*Mon compte – vue employés*" to manage citizen accounts. The Service de concertation des arrondissements has deployed a website for this purpose. The website provides access to procedures, guides and training for managing features of citizen accounts and related services. During interviews, however, we confirmed that the withdrawal of employee access rights is not systematic and is the responsibility of each business unit.

A lack of procedures for the periodic review and deletion of accounts could lead to non-uniform practices in the performance of those tasks. This could result in unauthorized access to sensitive information by some users.

3.1.2.B. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information formalize management frameworks for the periodic review and deletion of GIA Citoyens accounts and ensure that they are distributed to the stakeholders.

3.1.3. Centralized Identity and Access Management Strategy

When planning and implementing IAM, it is essential to establish an overall strategy that involves all stakeholders. The components of a good strategy include:

- Scope of the project;
- Business needs;
- Software benchmarking;
- Standards and best practices;
- Current and target architectures.

GIA Employés

- ***Current Status of the Project***

After the GIA Employés project was launched in 2016, it was impacted by the departure of key employees, including the business and security solutions architects and the delivery manager. Those departures created issues around project continuity and standardization of the work. In addition, the committee initiative, with the involvement of business units, was abandoned.

As a result, the current project is focused on technology and therefore prioritizes:

- Software benchmarking;
- Delivery of tools to improve authentication;
- Deployment of infrastructure in all environments for the selected tools;
- Documentation of the architectures and RASCI responsibility matrices for each tool.

The following mechanisms have been put into operation:

- The two-factor authentication;
- Single sign-on. This allows users to access several applications based on a single authentication;
- Requirements for more complex passwords.

Nevertheless, the lack of detailed documentation of architectures (current and target), the technology in place, as well as the needs and risks, have led to major issues, including:

- Delayed detection of the incompatibility of the former directory with the new one;
- The high cost of supporting the authentication tool, preventing an update to the latest version;

- The tool selected for the centralized governance and management of identities was abandoned;
- The need to re-evaluate the high-privilege accounts solution due to issues pertaining to support and functions.

Given the current situation, the project has slipped into emergency mode. The team is working to correct the situation and reviewing the IAM strategy.

- ***Project Scope***

Documents provided by the project team concerning this criterion include:

- The roadmap for the IT security and continuity program (approved in 2018), whose scope takes into consideration:
  - All users (employees and external resources) except for citizens;
  - All hardware assets representing an access point (such as servers, printers and workstations);
  - All software assets (including databases, applications and Internet services);
- The identity management project charter (approved in 2020) contains inconsistencies between certain sections pertaining to user types. In the purpose, for example, all users and connected systems are listed, whereas in the table of end users, only elected officials, employees, interns and outside consultants are included.

We observed that the initial scope concerning the population served changed in 2020. It is now ambiguous and does not formally list all the identities managed by the City (e.g., business partners, suppliers, and physical and software assets).

As for deliverables, the new project charter identifies the requirements for the new solution (including architecture documents, technological solutions and target processes). We noted, however, the lack of:

- Documentation of business needs;
- Documentation about use cases that demonstrate the operational relationship between the stakeholders and the IAM;
- A detailed analysis of the processes and technologies already implemented;
- Issues and constraints that the project needs to take into consideration.

- ***Overall Strategy and Business Needs***

Organizational Commitment

IAM is a process that requires the support of senior management and the commitment of various business units. The directive concerning logical access management states that the adoption of a global approach to access management is the responsibility of the CSI. The CSI should therefore have formal ongoing

involvement in the IAM project. However, we found that the only meeting with the committee about access management took place in January 2020. The minutes show that discussions took place concerning the new directive addressing logical access management but that the roles and responsibilities of the CSI in terms of access management were not presented.

Project Phases

In reviewing the roadmap for the IAM project, which details the main implementation phases, we observed that:

- The deficiencies mentioned in the project charter (project scope section) are also reflected in the roadmap;
- Process activities are related to technological tools, and there's no activity for IAM processes as a whole;
- No follow-up (progress and tasks completed) is specified for related activities;
- Standardization of the activities for each project phase is lacking. For example:
  - Activities related to the GA access tool were not completed;
  - For the high-privilege accounts solution, release activities has preceded process documentation.

These deficiencies do not allow to fully respond to the scope of the project and the needs of users.

- ***Software Benchmarking***

A first software benchmarking for IAM took place in 2016 and was updated in 2020. The compliance of several products with identified functions was evaluated. The benchmarking showed that the access authentication and management tool selected and implemented did not fully meet the City's needs.

Finally, in 2021, the STI conducted a new benchmarking that only includes the selected technological tool's functions.

The team may therefore once again end up selecting a solution that does not include all the functions identified in the earlier benchmarking, which would result in shortcomings with respect to the objectives of the IAM project.

- ***Standards and Best Practices***

The document "*Contexte et impacts de la GIA*" lists the laws and management frameworks requiring compliance. The architecture documents for the directory and the access and authentication management tools also refer to the City's internal directives, guides and standards.

However, these documents do not mention standards or best practices for IAM such as the *National Institute of Standards and Technology (NIST)* or the pan-Canadian identity management framework of the Digital ID & Authentication Council

of Canada (DIACC).[2] These standards establish control mechanisms and security requirements specifically for IAM in accordance with the security and sensitivity levels of the assets being accessed. They would enable the City to implement standardized IAM infrastructure and processes that ensure satisfactory protection of its information assets.

- ***Current and Target Architectures***

No document currently exists about the overall IAM architecture (current and target), including identities, services and their interaction. The architecture documents provided are specific to each technological tool and present only the components with which each solution interacts.

In conclusion, deficiencies in the City's IAM strategy could have a significant impact on IAM, making it non-standardized and insecure and thereby depriving users of a coherent and simplified access to information assets. These shortcomings could eventually result in needs not being met, incomplete processes and procedures, and technological tools lacking the necessary features. Moreover, the lack of information and interaction with CSI may lead to a failure to:

- Adopt a cross-sector approach to standardize access management across all business units;
- Properly manage the risks associated with logical access management;
- Ensure collaboration among the various stakeholders in effectively implementing best practices for access management.

3.1.3.A. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information specify the scope of the project and ensure that the following components are included:

- User types;
- All deliverables pertaining to the current and target situations (management frameworks, processes and technologies).

3.1.3.B. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information ensure that the Comité de sécurité de l'information is aware of and assumes its responsibilities as set out in the Directive de gestion des accès logiques.

[2] The Trust Framework Expert Committee (TFEC) of the Digital ID & Authentication Council of Canada (DIACC) has been developing the Pan-Canadian Trust Framework™ since 2016.

3.1.3.C. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information ensure the standardization of all milestones in each phase of the Centralized Identity and Access Management project.

3.1.3.D. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information integrate the following components into the project strategy:

- An analysis of the technological context and current processes;
- The business needs and use cases of the different business units.

3.1.3.E. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information integrate the identified business needs and functions into the software benchmarking.

3.1.3.F. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information formally specify the best practices adopted as part of the Centralized Identity and access Management project.

3.1.3.G. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information define the current and target architectures for all Centralized Identity and Access Management processes.

GIA Citoyens

- ***Project Scope***

The project known as DCI meets the needs of citizens and integrates their digital identity. The scope includes mechanisms for managing citizen identities and access in accordance with the services they request. Citizen identities also take into consideration their relationships with businesses. Moreover, the project team plans to address the user needs of citizens in terms of family groups (e.g., parents and children).

As for the implementation of the authentication tool, its functional scope is properly defined in the architecture document, including the use cases.

- ***Overall Strategy and Business Needs***

We found that the current DCI architecture has a global perspective that accurately represents the current situation. It presents a high-level view of citizens' interactions with the systems that provide them with services.

For the target architecture, the steps to be followed are laid out with priorities for integrating services into the DCI portal in accordance with the population served.

- ***Software Benchmarking***

The same solution is used for managing the identities of both citizens and employees. No benchmarking specific to GIA Citoyens exists.

- ***Standards and Best Practices***

The project has adopted the Pan-Canadian Trust Framework (of the DIACC) for determining the required assurance levels when identifying a citizen. However, implementation is still ongoing.

Furthermore, when integrating applications into the single sign-on used by GIA Citoyens, the project team adopted an international industry standard.[3] This standard authorizes applications to verify an end user's identity based on the authentication provided by GIA Citoyens through a simplified, standardized process.

- ***Current and Target Architectures***

The current and target IAM architectures are documented appropriately in the material we audited. In addition, technical aspects are duly formalized, which allows for a better understanding of the solution in place.

We consider that the various documents pertaining to the GIA Citoyens strategy are adequate.

No recommendation is necessary.

3.1.4. Risk Analysis

An IAM risk analysis determines the requirements and controls that need to be implemented to protect user identities and access to the City's assets. Specific controls are determined according to the level of confidentiality, integrity and availability of the information being accessed.

Assurance levels are established in order to define the minimum security requirements needed to identify and authenticate users, as well as the integration of new applications. These are determined in accordance with the risk level of the information being accessed. When identifying users, for example, the lowest level does not require any proof of physical identity. For the highest level, on the other hand, users must come in person and provide valid documents proving their identity.

---

[3] OIDC: OpenID Connect is a standard managed by the OpenID Foundation. It is a single-layer authentication that verifies the identity of users.

GIA Employés

We audited the risk analysis and its action plan and noted the absence of:

- Formal adoption of IAM security standards;
- Formal adoption of assurance levels for identification, authentication and application integration;
- Mitigation measures pertaining to centralized IAM technologies (e.g., centralized access management by profile);
- Information concerning the residual risk in various situations following implementation of the proposed measures;
- Timelines with assigned responsibilities.

In the absence of an adequate risk analysis, the control mechanisms in place may not be adapted to the risk level of information assets. This means that significant IT risks may not be sufficiently mitigated (e.g., confidential or personal information being compromised).

3.1.4.A. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information formally establish assurance levels for the identification and authentication of users, as well as for the integration of applications into Centralized Identity and Access Management.

3.1.4.B. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information ensure that the risk analysis proposes mitigation measures based on the technologies used for the Centralized Identity and Access Management project, as well as on standards adopted by the City.

3.1.4.C. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information ensure that the mitigation measures implemented comply with the assurance levels established for identifying and authenticating users, as well as for the integration of applications into Centralized Identity and Access Management.

3.1.4.D. Recommendation

We recommend that, for GIA Employés, the Direction sécurité de l'information of the Service des technologies de l'information ensure that the action plan provides for follow-up to the implementation of the proposed mitigation measures.

GIA Citoyens

We obtained a document listing the main security risks together with a list of generic mitigation measures that are part of good security practices used by the industry but that are not formally related to the controls implemented in the GIA Citoyens project. Moreover, our analysis of the document shows that following are missing:

- The impact of the risks identified and their likelihood of materialisation;
- The implementation status of the proposed mitigation measures;
- An action plan concerning the mitigation measures to be implemented, including a timeline and assigned responsibilities.

The project team has produced a map of the personal information associated with the DCI. While this work includes recommendations, most of them do not yet have an expected resolution date.

The STI explained to us that the impact and risk analyses have not yet been conducted due to a lack of resources. However, the team has begun work to implement security controls.

GIA Citoyens adopted the Pan-Canadian Trust Framework (of the DIACC) in establishing the assurance levels required when identifying citizens who request access to services, and the standard is currently being implemented. The GIA Citoyens team is considering aligning itself with a pan-Canadian identity, but the project is still under analysis.

In the absence of an adequate risk analysis, the control mechanisms in place may not be adapted to the risk level of information assets. This implies that the IT risks may not be adequately mitigated (e.g., compromise of confidential information).

3.1.4.E. Recommendation

We recommend that, for GIA Citoyens, the Division solutions numériques of the Service des technologies de l'information conduct a risk and impact analysis.

3.1.4.F. Recommendation

We recommend that, for GIA Citoyens, the Division solutions numériques of the Service des technologies de l'information formalize assurance levels for the identification and authentication of users as well as application integration into Centralized Identity and Access Management.

3.1.4.G. Recommendation

We recommend that, for GIA Citoyens, the Division solutions numériques of the Service des technologies de l'information ensure that the mitigation measures in place comply with the assurance level established for the identification and authentication of users as well as application integration into Centralized Identity and Access Management.

3.1.4.H. Recommendation

We recommend that, for GIA Employés, the Division solutions numériques of the Service des technologies de l'information establish an action plan to follow up the proposed mitigation measures.

3.2. User Management (Identities)

Centralized user management manages accounts, as well as roles and identities, from provisioning through to deactivation. This includes high-privilege accounts requiring stronger mechanisms to protect them against illegal actions.

GIA Employés

Based on the information collected, user management is decentralized and does not, strictly speaking, constitute an IAM system because:

- Current user management (provisioning, review, withdrawal, modification and deactivation) responds to administrative processes originating from different business units;
- The main IAM components are not integrated into a single management tool and the processes are not centralized;
- The criteria and requirements for creating, reviewing, withdrawing, modifying and deactivating the different account types are not standardized. For example:
  - Creating accounts for external users requires only their name and email address. If a contract has no deprovisioning date, the account is assigned a default lifetime of two years;
  - Account provisioning for employees follows a process, formalized by the SRH, which verifies the identity of new employees and leaves a trace in the system. When an employee leaves, his account is automatically deactivated.

Furthermore, the project team:

- Plans to implement a new directory to replace the old one which is still in production;
- Will replace the profile governance and management tool that was selected at the beginning of the project;
- Recently implemented a password vault for the management of high-privilege accounts, which is being re-evaluated.

We will not issue a new recommendation since the recommendations in section 3.1.4. already cover the areas for improvement, and the identity management tools in place will be replaced at some point.

GIA Citoyens

- ***Citizens Web Interface***

With respect to the life cycle of citizen identities, the centralized mechanisms are sufficient and standardized for the following:

- Registration and verification of user identities;
- Account deprovisioning (at the citizen's request);
- Account deactivation (temporary following a prescribed number of unsuccessful login attempts).

However, we did not find any mechanism for deprovisioning inactive accounts. This means that a citizen account is removed only at their request through a manual process.

The only high-privilege account is managed by the GIA Citoyens administrator, who is an employee. For this administrator, the team plans to adopt the high-privilege account solution that will be part of GIA Employés. Citizen accounts do not have high-privilege rights. Accounts used for applications also have restricted access.

Inappropriate management of the life cycle of accounts could result in lost, stolen or compromised data or forged identifiers.

3.2.A. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information implement mechanisms in GIA Citoyens to deactivate and delete inactive citizen accounts.

3.3. Authentication Management

IAM standardizes authentication methods and reduces the multitude of passwords required to access systems. This simplifies life for users and reduces the risk of unauthorized access. Moreover, IAM provides standardized authentication methods adapted to the level of risk of the information being accessed. For example, parameters for password authentication settings must be aligned with the City's policy (e.g., minimum password length, the inclusion of uppercase and special characters, and the rejection of previously used passwords). In addition, granting access to critical assets requires the implementation of multifactor authentication (e.g., something users know (a secret) and something they possess (such as a telephone or physical access card)).

In order to detect unauthorized access attempts, every organization must have an access monitoring process. It also provides for a more effective analysis should an access incident arise.

GIA Employés

The IAM tool in place integrates two-factor authentication with an industry-recognized solution. Efforts have also been deployed to enhance password complexity. As we mentioned in section 3.1.4. of the report, risk analysis and assurance levels have not been completed. For this reason, the authentication methods in place are not in line with the risk level of the assets being accessed.

As for logging and monitoring, access logs are maintained but work is in progress to integrate them into the centralized log management tool.

We will not issue a new recommendation since the recommendations in section 3.1.4. already cover the areas for improvement, and the tool used for authentication will be replaced.

GIA Citoyens

- ***Citizens Web Interface***

In order to simplify access for citizens, the authentication method implemented requires only a password with a cellphone number and email address to validate the citizen's account. There is no multifactor authentication. There are, however, mechanisms that reduce the risk of compromise, including the temporary deactivation of accounts following a fixed number of unsuccessful login attempt.

As indicated in section 3.1.4. of the report, risk analysis and assurance levels have not been completed, and authentication is not adapted to the various risk levels. Currently, certain settings in authentication method, including password complexity, do not comply with the City's logical access management standard.

- ***Employees Web Interface***

Employees accessing GIA Citoyens use their GIA Employés authentication. As a result, authentication management in such cases is handled by GIA Employés.

As for logging and access monitoring, logs are saved in the DCI infrastructure and also sent to the centralized log management tool. They are properly structured and allow for searches to resolve incidents.

3.4. Access Management

IAM includes mechanisms for approving, granting, modifying, withdrawing and reviewing access privileges. These features foster compliance with security best practices, such as the least-privilege and need-to-know criteria. In this context, the assignment of high-privilege accounts also needs to be regulated and more closely monitored.

IAM also simplifies the periodic review of access rights to detect modifications in user assignment.

GIA Employés

Based on the information collected, access management is currently decentralized rather than being managed around a central solution. Strictly speaking, it therefore does not qualify as IAM.

According to the roadmap, an access management tool has not yet been selected. There is no automated mechanism for integrating rules regarding the segregation of duties, least privilege or incompatible authorizations.

Furthermore, during meetings with the stakeholders, they confirmed that access management is under the responsibility of each business unit and based on administrative processes.

Finally, no centralized, standardized mechanisms are in place for the periodic access review.

We will not issue a new recommendation since the recommendations in section 3.1.4. already cover the areas for improvement, and a technological tool is not yet in place.

GIA Citoyens

- ***Citizens Web Interface***

The system provides citizens with basic access, and further access rights are granted on an as-needs basis when additional services are requested. By default, therefore, access management complies with the principles of need-to-know and least-privilege.

- ***Employees Web Interface***

To perform maintenance and support operations for the services offered to citizens, employees access the DCI environment. To obtain such access, they use the appropriate form to file a request with the Service de concertation des arrondissements. Requests can therefore be made to grant or withdraw employee access to DCI and related services. However, responsibility for periodic access review and withdrawal lies with each business unit and is not conducted systematically.

Given the absence of a process for periodic access reviews, the City faces an increased risk of inappropriate or unnecessary access to some information assets that are not in line with the employee's job responsibilities.

3.4.A. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information implement a process to periodically review access to GIA Citoyens.

3.5. Application Integration into Centralized Identity and Access Management

Integrating new applications into IAM reduces the number of authenticators users need and simplifies the integration of authentication into applications. The use of a formalized written procedure makes application integration more seamless and better standardized.

GIA Employés

A summary procedure is available for the integration of applications into IAM. The project team has already integrated about 125 applications, most of which use a second factor. Every integration involves the support of the security team. This procedure should be adapted to the project's new circumstances moving forward.

We will not issue a new recommendation since the recommendations in section 3.1.4. already cover the areas needing improvement.

GIA Citoyens

An examination of the process for integrating new applications into IAM shows that two teams are involved. The first manages the DCI portal, and the second, the GIA Citoyens infrastructure. During our audit, we observed that:

- The DCI form recently implemented meets operational needs and corresponds to the IAM vision. It contains the functional requirements to ensure proper integration into the DCI portal. The Division solutions numériques team manages requests;
- The integration of applications into GIA Citoyens is based in an automated process and is duly authorized by the IAM administrator.

The team managing the DCI aims to become the master source for citizen access. However, the GIA Citoyens integration form does not request any information about DCI integration. During meetings, it was confirmed that this aspect is not systematically evaluated.

Application integration is not adapted to the various risk levels. We already indicated in section 3.1.4. of the report that risk analysis and assurance levels have not yet been completed.

The impacts of this deficiency with respect to application integration on the City are:

- Lack of standardization and visibility pertaining to access rights granted to citizens by the DCI;
- Access management that is not fully centralized;
- Actions taken by citizens on applications connected only to GIA Citoyens that are not traceable.

3.5.A. Recommendation

We recommend that the Division solutions numériques of the Service des technologies de l'information ensure that applications integrated into GIA Citoyens are also integrated to the Dossier citoyen intégré and that any exception is formally justified.

4. Conclusion

The Ville de Montréal (the City) initiated two projects in response to the needs of employees and citizens for Centralized Identity and Access Management (IAM). This resulted in the implementation of two distinct solutions, one for citizens and the other for employees.

On the whole, GIA Citoyens does not present any major risk to the confidentiality, integrity and availability of data. The control mechanisms in place demonstrate sound IAM. The strategy is appropriate and takes into consideration both the current situation and the long-term vision. The access granted to citizens meets the least-privilege and need-to-know principles. Nevertheless, in our opinion, the work in progress to adopt the Pan-Canadian Trust Framework for digital identities needs to continue. This would allow the integration of standardized control mechanisms, recognized by the industry, for the protection of personal information and the security of services offered to citizens.

On the other hand, since the GIA Employés project is being relaunched, several criteria could not be evaluated. We concentrated our audit work on project governance and identified major deficiencies, such as the consistent lack of involvement of the Comité de sécurité de l'information (CSI), as well as the absence of a process owner and overall strategy. The risk analysis and proposed mitigation measures do not qualify as IAM. Currently identified controls are, in fact, decentralized, administrative mechanisms. Consequently, the technological solutions and processes in place do not ensure adequate risk management regarding the confidentiality, integrity and availability of IAM data. Nevertheless, efforts have been deployed to integrate applications into IAM and to enhance authentication security. Despite the shortcomings, those efforts have allowed users to reduce their number of passwords.

The City does not yet have a solution to centralize employee identities and access.

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

Evaluation Criterion – Governance

Concerning GIA Citoyens:

The GIA Citoyens owner process has not been formally identified and the associated role and responsibility matrices have not been finalized or formally approved.

On the whole, the management frameworks for GIA Citoyens are adequate except for those applicable to the periodic access review and account deletion, which are missing.

The GIA Citoyens strategy is properly documented and includes all the main components:

- Project scope;
- Overall strategy and business needs;
- Standards and best practices;
- Current and target architectures.

The risk analysis does not assess the impact of risk scenarios or their likelihood of materialisation. Moreover, there is no action plan for the mitigation measures to be implemented. Finally, assurance levels for identification, authentication and application integration into IAM have not been formally established.

Concerning GIA Employés:

The IAM process owner at the City has not been formally identified, and the associated role and responsibility matrices have not been documented.

The management frameworks and processes specifically used in IAM have not been completed or formalized.

The GIA Employés strategy presents a number of shortcomings:

- The scope with respect to user types has not been defined;
- The CSI and business units are not involved on a regular basis;
- The project phases and deliverables are not aligned;
- The analysis of the current context (processes and technologies) and business needs are not documented;
- Software benchmarking has not integrated business needs and the identified functions;
- IAM standards and best practices have not been formally adopted;
- Current and target architectures are missing.

The risk analysis is incomplete and the mitigation measures are not aligned with an IAM system and industry standards. Furthermore, assurance levels for the identification, authentication and application integration into IAM are not formally defined.

Given that the project is being relaunched and that the current technological tools will be replaced, we did not evaluate other criteria initially established as within the scope of this audit. Nevertheless, we issued recommendations in section 3.1.4. that can be used to improve aspects of the criteria that were not evaluated:

- User management (identities);
- Authentication management;
- Access management;
- Integration of applications into IAM.

Evaluation Criterion – User Management (Identities)

GIA Citoyens users are properly managed apart from the lack of a mechanism for deleting accounts.

Evaluation Criterion – Authentication Management

We found that authentication management in GIA Citoyens is not yet adapted to assurance levels that establish security requirements in accordance with the degree of confidentiality of the information being accessed.

Evaluation Criterion – Access Management

Access management in GIA Citoyens is adequate. However, in the case of employees accessing citizen records, responsibility for the periodic review and withdrawal of access rights lies with each business unit and is not conducted systematically.

Evaluation Criterion – Application Integration into Centralized IAM

The application integration process for GIA Citoyens is adequate on the whole, but the teams do not systematically ensure that applications integrated into GIA Citoyens are also in the Dossier citoyen intégré (DCI) and that any exception is formally justified. In addition, application integration needs to be adapted to the assurance levels set out in section 3.1.4.

5. Appendix

5.1. Objective and Evaluation Criteria

Objective

To determine whether the Centralized Identity and Access Management (IAM) process and the related control mechanisms put in place by the Ville de Montréal (the City) ensure that they present no major risk to the confidentiality, integrity and availability of data.

Evaluation Criteria

Criterion 1: Governance
The IAM governance in place is properly documented and includes a definition of roles and responsibilities, policies, management frameworks, a strategy, and a risk analysis that establishes requirements and controls to be implemented.

Criterion 2: User Management (Identities)
Secure mechanisms for managing user identities and privileged accounts are in place. They cover the account life cycle from provisioning to deprovisioning.

Criterion 3: Authentication Management
Digital authentication mechanisms consistent with industry best practices are in place and correspond to the risk level of the information assets requiring protection.

Criterion 4: Access Management
Access management is handled in accordance with security best practices (e.g., the principle of least privilege, separation of duties and periodic revision of access).

Criterion 5: Application Integration into Centralized IAM
The integration of applications belonging to the City or third parties into IAM authentication functions follows a formally established and standardized procedure.