



Report of the Auditor General of the Ville de Montréal to the City Council and to the Urban Agglomeration Council

For the Year Ended December 31, 2012

“Time Management” Subproject

5.12

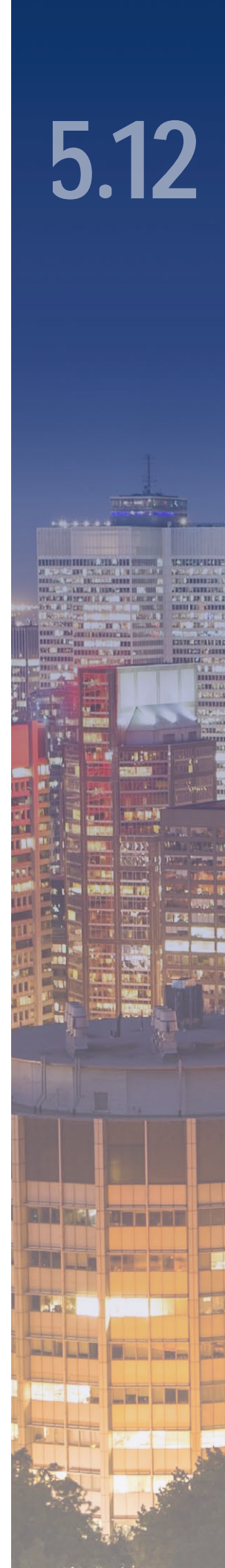


Table of Contents

1. Introduction	471
2. Audit Scope.....	472
3. Findings and Recommendations	473
3.1. “Time Management” Subproject Governance	473
3.2. Development Phases	477
3.3. Security	485
3.4. Performance.....	490
3.5. Evolution of the Kronos Platform.....	492
3.6. Continuity Plan	493

List of Acronyms

CCGPE	Comité corporatif de gestion des projets d'envergure	LDAP	Lightweight Directory Access Protocol
CMPE	Comité de monitoring des projets d'envergure	POM	project organization manual
CSTI	Comité sectoriel des technologies de l'information	SCHC	Service du capital humain et des communications
DRPTI	Division réalisation de projets TI	STI	Service des technologies de l'information
		TM	time management

5.12. “Time Management” Subproject

1. Introduction

Time management (TM) was already a concern in 2000, when the Ville de Montréal (the city) issued a first call for tenders for the purchase of a computerized work attendance management and data collection system.

Thereafter, in 2004, as part of the SIMON (*Système Intégré Montréal*) program adopted by the executive committee on October 8, 2003, the city launched the Integrated HR-Payroll MS project, which was aimed mainly at providing the city with an integrated management system to support human resources and payroll management processes based on the best practices of large organizations. The processes included in the scope of the initial Integrated HR-Payroll MS project included the TM process, hereinafter referred to as the “TM subproject.”

In July 2006, a moratorium was announced for the SIMON program and all work on the HR-Payroll MS project was interrupted. By then, the city had purchased the Kronos software package after analyses had shown that the Oracle Suite did not provide the necessary functions to enable the city to manage its TM process efficiently. At the time, work on the TM subproject was under way only in the Lachine and LaSalle boroughs, the wastewater treatment plant and the Centre d’urgence 911.

In April 2007, work on the TM subproject resumed under the responsibility of the Service des finances, which separated the subproject from the SIMON program. At that time, the purpose of the project was to *[TRANSLATION] “provide the city with a single time management system to enable all boroughs and city departments to manage work attendance, work schedules, time banks and time transfers between cost centres locally in order to gather payroll information while managing its time management process more efficiently¹.”*

Meanwhile, the TM subproject continued and, at the end of our audit work, the subproject’s two phases had progressed as illustrated in Table 1.

¹ Project organization manual, *Gestion de temps – Kronos*, phase 1, May 20, 2007.

Table 1 – TM Subproject Progress

Phase	Scheduled date	Actual date
1. Pilot deployment for certain groups of employees in the Lachine, LaSalle, Ville-Marie and Mercier–Hochelaga-Maisonneuve boroughs as well as the wastewater treatment plant and the Centre d'urgence 911	February 2008	May 2008 ^a
2. Deployment for all other employee groups apart from police officers and firefighters ^b	May 2009	December 2012

^a Partially completed and transferred to phase 2.

^b Originally, police officers and firefighters were included in phase 2.

At the end of our audit work, we were informed that the Kronos software package would be deployed for firefighters during the first half of 2013. As for the police officers, no deployment date had yet been set.

2. Audit Scope

Initially, our audit dealt only with the work carried out under the TM subproject. However, considering that the TM subproject is based on the Integrated HR-Payroll MS project and that—following the moratorium announced in July 2006—the revival of this subproject remained both uncertain and challenging at the time of our audit, we decided to extend the scope of our audit to include the project's then current status.

Since the scope of analyzing the status of the Integrated HR-Payroll MS project is in no way comparable to conducting an analysis of the TM subproject's status, we decided to tackle each of these analyses in separate audit reports. This audit report therefore addresses only the TM subproject. In this regard, given the delays observed with respect to the implementation of the Kronos software package, we set the following objectives for our audit:

- assess the current management of the TM subproject regarding the implementation of an efficient TM system;
- take stock of current risks with respect to business continuity, compliance remunerated TM framework and the efficient management of related operations.

We conducted most of our audit work between October 2011 and June 2012, and our audit included a global review of the key aspects of the TM subproject since its launch in 2005. However, we updated certain data inherent to the level of advancement of the TM subproject as at December 31, 2012.

Note that the choice of the Kronos software package to support TM process management was not included in the scope of our audit. Furthermore, we focused our work such as to evaluate whether or not the processes in place enabled the configuration of the Kronos software package in compliance with collective agreement provisions and other frameworks determining work conditions. Our intention was not to conduct an extensive evaluation of the level of compliance of the data thus configured.

3. Findings and Recommendations

It must be pointed out that, at the time of our audit, the Service des technologies de l'information (STI) was in the process of implementing a new information technology project management framework. In principle, this framework should mitigate the risks of future projects being hindered by the same problems as those described in this audit report. We shall cover the application of this framework in upcoming information technology project audits.

3.1. “Time Management” Subproject Governance

3.1.A. Background and Findings

A project organization that includes the required resources and an efficient decision-making structure must be combined with rigorous risk management procedures to ensure the project's successful outcome.

Project Governance Structure

Our audit work found many organizational changes made to the TM subproject's governance structure, those changes having stemmed from the Integrated HR-Payroll MS project.

First the moratorium announced for the SIMON program in July 2006 had impacts on the monitoring of the TM subproject. At the time this moratorium was announced, the Service du capital humain was this subproject's proponent and was acting as the owner of the TM process. In April 2007, the Service des finances took over the TM subproject which it managed as both proponent and mandatary until June 2011. From that moment on, the STI took over as the subproject's mandatary, acting on behalf of the Service des finances.

Second, our audit work found that the project organization manuals (POMs) for phases 1 and 2 simplified the governance structure initially developed for the Integrated HR-Payroll

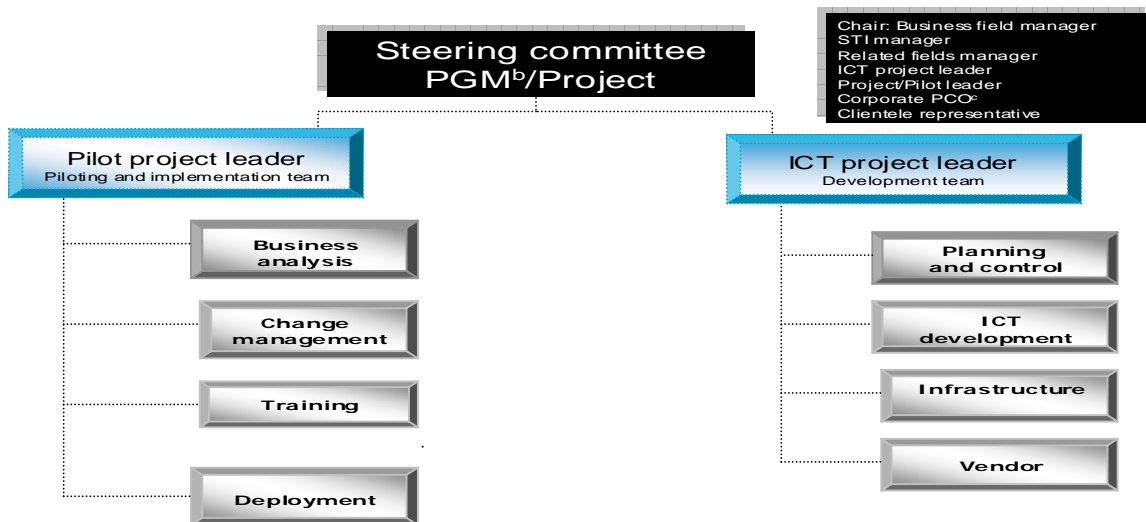
MS project. We must emphasize that this structure made no provision for a coordination committee although such a committee was needed to create synergies between the project delivery teams and thus favour an efficient deployment of the TM subproject. Furthermore, we note that the steering committee's hierarchal structure does not endow members with the authority they need to intervene and make the necessary decisions to ensure that the TM subproject unfolds smoothly.

During the completion of phases 1 and 2, which spanned from April 2007 to the beginning of 2011, the anticipated governance structure was modified several times as were the composition and roles and responsibilities of the steering committee and follow-up committee. Furthermore, the members of these committees met less and less often, to the point where the steering committee met only once in 2010 and 2011 and the follow-up committee held no meetings whatsoever during this period.

The TM subproject participants who we met informed us that these governance gaps hindered the completion of the project in several ways and that the TM subproject was basically left unchecked during this period.

However, during the course of 2011, a new governance structure was implemented for the TM subproject (see Figure 1) and a new project leader was appointed. Thereafter, we observed a gradual improvement of the situation.

Figure 1 – ICT Project Governance Model^a



^a Information and communications technologies.
^b Combined management model for the program and project.
^c Project control officer.

Process (or system) ownership is a universally accepted principle of sound management. In fact, the process or system owner plays an important role in the governance and completion of a project. The owner chairs the project’s steering committee and specifically must:

- justify the project and account for the realization of expected benefits;
- authorize the implementation of the solution and organizational changes;
- ensure that the project is planned such as to incorporate his or her business field’s current activities.

The TM process owner was never officially announced while the TM subproject was being carried out. Several arguments justify giving ownership of this sub-process to the Service du capital humain et des communications (SCHC). Indeed, the SCHC negotiates, states and enforces the rules pertaining to TM. Moreover, the SCHC played that role during the period preceding the revival of the TM subproject by the Service des finances in April 2007.

However, the TM subproject has been managed by the Service des finances since it resumed in April 2007. Furthermore, the Kronos software package that supports the TM process contains parameters that are inherent to work conditions and that constitute the payroll process’ main input. Consequently, the TM process is similar to a financial process and the Service des finances can admittedly claim ownership of it.

Ultimately, the owner of the TM process must be officially designated in order to clear up the roles and responsibilities as well as resulting accountability issues. After this audit report was confirmed with the business units concerned, the Service des finances was appointed owner of the TM process.

Risk Management and Accountability

Although the POMs for phases 1 and 2 set out certain technological and organizational risks, no concrete measures were taken to mitigate them and these risks were never updated or integrated into a formal follow-up and accounting structure during the project’s implementation. Moreover, the risks referred to in the phase 1 POM are the same as those referred to in the phase 2 POM.

This established fact—combined with the deficiencies presented earlier in the chapter on governance—admittedly contributed to the loss of control over the TM subject’s implementation timeline as well as to the difficulties experienced by the project team while searching for solutions to certain problems. Among other things, the failure to take into consideration from the outset the impacts of integrating the payroll systems of boroughs

created from former suburban municipalities into the city's system as well as the individual characteristics of their respective pension plans speaks volumes to this effect.

3.1.B. Recommendation

We recommend that the Service des finances, owner of the process, and the mandatory of the “time management” subproject, namely the Service des technologies de l'information, identify their respective risk management and reporting responsibilities, integrate the subproject's current risks into a single dashboard, ensure systematic follow-up and report thereon to the steering committee and the Comité sectoriel des technologies de l'information.

Business units' responses:

SERVICE DES FINANCES

[TRANSLATION] At present, a monthly dashboard is sent to the Comité sectoriel des technologies de l'information (CSTI); also a follow-up table for major projects is sent to the Comité corporatif de gestion des projets d'envergure (CCGPE) and to the Comité de monitoring des projets d'envergure (CMPE) by the Division réalisation de projets TI (DRPTI) of the STI. The dashboard includes an updated risk assessment for the project.

The dashboard is submitted for approval by the head of the steering committee of the Service des finances before being sent to the CSTI.

Risks are systematically monitored to identify appropriate mitigation measures, which are indicated in the monthly dashboard. (Completed, April 2013)

SERVICE DES TECHNOLOGIES DE L'INFORMATION

[TRANSLATION] At present, a monthly dashboard is systematically sent to the CSTI; also a follow-up table for major projects is sent to the CCGPE and the CMPE by the DRPTI of the STI. The dashboard includes an updated risk assessment for the project.

The dashboard is systematically submitted for approval by the head of the steering committee of the Service des finances before being sent to the CSTI.

Risks are systematically monitored to identify appropriate mitigation measures, which are indicated in the monthly dashboard. (Completed, April 2013)

3.2. Development Phases

3.2.1. Implementation Strategy

3.2.1.A. Background and Findings

The TM subproject implementation strategy was based on a gradual implementation schedule. Initially, the project was split up into two phases.

Phase 1 provided among other things:

- review of the architecture;
- migration (seeing as the city was already using the Kronos package) of the solution, for the “blue collar” category only, to the Ville-Marie and Mercier–Hochelaga-Maisonneuve boroughs;
- review of the analysis conducted to replace “GesHor” (the schedule management system currently used by the wastewater treatment plant) by Kronos;
- review of the analysis conducted to replace the time recording function then handled by Kronos’ Athena application;
- implementation of Kronos, for the “blue collar” category only, in the LaSalle and Lachine boroughs;
- implementation of Kronos, for the “permanent white collar” category only, in the Centre d’urgence 911 and the wastewater treatment plant;
- training, deployment, support and acceptance of the deliverables for each borough and unit where the Kronos software package was implemented.

Phase 1, which ran from April 2007 to February 2008, was meant to provide an evaluation of the total cost of implementing the Kronos software package throughout the city as well as the proof of concept and lessons learned for the implementation of the second phase. As for phase 2, the goal was to complete all of the deliverables and the implementation of the system for all city employees, with the exception of the firefighters and police officers. This second phase was scheduled from January 2008 to January 2009.

The post-mortem conducted on phase 1 shed light on several major problems that had arisen during the development and implementation of the components making up the Kronos software package. Indeed, the post-mortem documents reveal that the deliverables were only partially completed, that work was not always completed according to schedules, that the total cost of the project had not been evaluated and that several planned programming operations had been postponed to phase 2. Furthermore, comments issued during the post-mortem testified to several deficiencies (e.g., the instability of the system,

last-minute modifications and duplicate data entries, which significantly increased the workload and delayed the implementation of the system).

Moreover, the chosen deployment strategy—i.e., to transfer only some of the users within a same unit during phase 1 of the TM subproject—emphasized the difficulties encountered. Among other things, the strategy required a lot of training and support, practically as much as if all users had been converted to the new system. Maintaining the former TM systems for a portion of the employees also contributed to increasing the workload.

In our opinion, this situation is primarily due to the aforementioned gaps in the governance mechanisms, with respect namely to project leadership and risk management, which made it impossible to efficiently handle contingencies. However, it must be noted that the corrective measures taken as of 2011 turned the situation around and that the implementation process was operating smoothly by the end of our audit work.

3.2.2. Preliminary and Functional Analyses

3.2.2.A. Background and Findings

The preliminary analysis is expected to determine the processes and data for which gaps exist with respect to the software package's standard functions. A decision-making committee is then expected to determine the required administrative and operational changes to ensure that the processes comply with the package's basic functions and, if applicable, set out the mandatory changes required to the package's configuration.

Although this is only a high-level summary evaluation, we were unable to track a single analysis conducted to determine the gaps between the TM processes in place and the standard functions of the Kronos software package for the TM subproject. A gap analysis is nevertheless particularly important in the case of complex projects that affect the entire organization, that are implemented within a decentralized organizational structure and that involve many linkages and dependencies.

Moreover, the TM process is basically a very simple process consisting of recording the time worked by individuals, having it approved by their respective managers and transmitting the data to the payroll department. The documentation presents the time recording and schedule management sub-processes as repetitive processes that are required for payroll management yet add little value in terms of organizational management. Consequently, several administrative units must use add-on software packages to meet their needs, for management information in particular. These add-on packages required

either an interface to connect them with the TM systems then in place or the repeated entry of the same data in the parallel and add-on systems.

The Kronos software package was purchased to partially or fully address these requirements. However, no analysis or evaluation had confirmed the feasibility of this objective. At the time of our audit, a decision had not yet been made as to whether or not to use the Kronos package's modules to meet these needs.

3.2.2.B. Recommendation

We recommend that the Service des finances, which owns the process, make a list of the gaps with respect to the project's initial objectives, the functions currently used, those under study and those that have been abandoned while taking into consideration the impacts of these choices. We also recommend that the Service des finances report on these items to the Comité sectoriel des technologies de l'information to enable the latter to make the appropriate decision under the circumstances.

Business unit's response:

[TRANSLATION] The list of discrepancies has been completed and includes the following items:

- *List of parameterized Kronos functions and discrepancies with respect to the objectives of business units;*
- *Customization of Kronos:*
 - *Customization,*
 - *Actions taken to harmonize with payroll operations,*
 - *Configuration of the interface output,*
 - *Contextual codes for the salaried employees' interface,*
 - *Contextual codes for the waged employees' interface;*
- *List of further improvements to be made. (Completed, March 2013)*

3.2.3. Acquisition of Licenses

3.2.3.A. Background and Findings

According to the Aberdeen Group, an international study group, software licensing is an expense that represents between 10% and 30% of a project's total cost and is the second highest expense, after labour, incurred to implement IT projects. Furthermore, Aberdeen states that license holders must pay recurring annual software maintenance and support fees that may represent anywhere from 10% to 25% of license costs.

The following table provides a summary of the number of licenses purchased and used as part of the Integrated HR-Payroll MS project and the TM subproject.

Table 2 – Licenses Purchased and Used

	Oracle HR-Payroll		Kronos	
Year	2008	2012	2008	2012
Number of licenses purchased	254,500	280,500	177,500	179,170
Number of licenses used	110,100	150,500	0	89,376
Ratio (used/purchased)	43.3%	53.7%	0.0%	49.9%

Most of the Oracle HRMS Payroll suite licenses were purchased in 2003 and a majority of the licenses used with the TM subproject’s Kronos modules were acquired in 2004. A study conducted by the STI on the impacts of the July 2006 moratorium establishes the annual recurring fees paid for license support at approximately \$2 million.

According to the initial schedule determined for the implementation of the HR-Payroll MS project, all processes were to be completed by May 31, 2007. Given the project’s current status, it is difficult to evaluate the number of licenses that will have been actually used, especially if certain modules are abandoned or replaced by new versions. The decision to purchase such a large number of licenses at the outset of the project had an important financial impact on the project’s cost. In our opinion, such a decision must be re-examined for future projects.

3.2.3.B. Recommendation

We recommend that the Service des technologies de l’information, in collaboration with the Direction de l’approvisionnement, assess the relevance of using a progressive acquisition strategy that takes changing needs into consideration in the calls for tenders it issues for the purchase of software package licenses to optimize acquisition and maintenance costs.

Business unit’s response:

[TRANSLATION] Several actions have been taken:

- *This recommendation was integrated into the project management framework process under the supervision of STI’s Section soutien aux projets to ensure that it is taken into consideration during project phases 2, 3 and 4;*
- *The head of the DRPTI sent a message to the manager of the Direction de l’approvisionnement requesting an evaluation of the relevance of a progressive*

acquisition strategy for every call for tenders in all projects requiring the acquisition of a commercial software package or commercial software;

- *The head of the DRPTI sent a message to all the section heads of the DRPTI requesting that they assess the relevance of a progressive acquisition strategy for every call for tenders in all projects;*
- *The manager of the STI sent a similar message to all members of the management committee and to the CSTI. (Completed, April 2013)*

3.2.4. Parameterization and Data Conversion

3.2.4.A. Background and Findings

The parameterization and configuration of the Kronos package's TM processes were to be carried out in compliance with the applicable collective agreements and employment contracts. Incidentally, in the subproject documents, we were able to retrace the analyses used to determine business needs. These analyses detail the conditions and required time management processes in accordance with agreement provisions, letters of agreement and other official documents.

The SCHC is responsible for the TM process framework. However, the responsibility for the daily management and application of the process is delegated to individual departments and boroughs. The executive committee also authorized the decentralization of certain borough responsibilities regarding human resources management (during its January 26, 2005 session, decision CE 05-0122). This decentralization increased the risks of TM activities being managed in a non-uniform manner. Incidentally, based on the information obtained, the TM conditions are not always interpreted and applied uniformly by the administrative units.

Generally, we noted that several "local" agreements were approved by the upper management level of the administrative units concerned and that the specific TM conditions and schedules were thus parameterized. However, we were unable to reasonably assess whether or not these specific conditions and schedules were compliant with the provisions of the collective agreements and other frameworks given the absence of comprehensive lists in that regard.

Besides the fact that these "local" agreements increased the amount of programming and testing needed to configure the Kronos software package, we also noted that the configuration conditions had been parameterized without necessarily having been validated in advance with the SCHC. Consequently, in our opinion, there remains a risk that the employment conditions parameterized in the Kronos package are not compliant with the collective agreements and related frameworks.

3.2.4.B. Recommendation

We recommend that the Service du capital humain et des communications take the necessary measures to ensure that the collective agreements and letters of agreement were properly interpreted and integrated into the Kronos software package.

Business unit's response:

[TRANSLATION] The SCHC, in collaboration with Service des finances, is in the process of organizing the RH-paie project. Teams are currently planning the work and identifying obligations under collective agreements, letters of agreement and current employee compensation practices in order to accurately determine project costs.

*When the current phase is completed in fall 2013, the project will be at the implementation stage, and the SCHC will take the opportunity to ensure that letters of agreement, collective agreements and current practices are properly applied and interpreted. A full review will be conducted before programming begins. **(Planned completion: December 2014)***

3.2.5. Management of Requests for Changes

3.2.5.A. Background and Findings

The organization must implement a process for entering, documenting, evaluating, authorizing and managing requests for changes in accordance with project objectives. Also, it must be possible to track the status of each individual request for changes at each step of the management process.

We noted that there was no formal process in place to manage requests for changes. In effect, each group (operational and IT) has its own ways of doing things. The lack of such a process leads to a disorderly management of requests for changes and inevitably increases the implementation teams' workloads as well as the risks of processing requests for changes that are not necessary, urgent or compliant or again of not processing other requests.

Moreover, we noted that a few changes that were less urgent, including certain customizations, had been made. Furthermore, certain changes had not been properly documented or did not seem to have been approved at the different stages of the management cycle. Also, it seemed to us that the users were not always informed of the changes made at the implementation stage. We also noted the lack of a global registry of

requests for changes and their respective statuses to ensure that all interventions were rigorously tracked.

However, we must emphasize that, at the time of our audit, the STI was preparing to implement a framework for requests for changes based on the Macroscopic methodology.

3.2.5.B. Recommendation

We recommend that the Service des technologies de l'information take the necessary measures to implement, as quickly as possible, a rigorous process for managing requests for changes.

Business unit's response:

[TRANSLATION] A registry of requests for changes was created by the project team in 2012. Every request for changes received by email and accompanied by a completed change request form approved by the functional team is automatically added to the registry.

Any request not meeting these three criteria is returned to the sender with instructions to complete the request as just described.

Every month, the registry is systematically presented to the project coordination committee, which comprises the head of the steering committee, the head of the Division de la paie institutionnelle and members of the Service des finances functional team.

This group must approve the registry of requests for changes and the assigned priority levels. Project deliverables are followed up in the same way.

*Since January 2013, a representative of the operational team has been attending meetings of the coordination committee so that follow-up will continue once the Kronos software package has been transferred to the operational team.
(Completed, April 2013)*

3.2.5.C. Recommendation

We recommend that the mandataire of the "time management" subproject, i.e., the Service des technologies de l'information, set up a global registry of requests for changes, verify that all required authorizations were obtained and review the priorities of the changes under way.

Business unit's response:

[TRANSLATION] Given that the project is nearly complete, the registry comprises a list of requests for changes that have been prioritized by representatives of the Service des finances (in accordance with the evaluation criteria they prescribed on the form). The coordination committee therefore authorized the representatives of the Service des finances to reprioritize requests for changes, should the need arise. (Completed, April 2013)

3.2.6. Tests

3.2.6.A. Background and Findings

The “functional tests” must be carried out by expert users in an organized environment and in accordance with a specific strategy. Processes must have been determined for each function such as to limit the extent of each test under a plan and a script². IT personnel needs to provide support and coaching to the functional resources to ensure test efficiency and quality. Finally, the functional team's expert users are those who have the ability to evaluate the expected results and authorize productions.

We noted the absence of a global strategy including the nature, scope and number of tests to be carried out. Furthermore, despite a very high number of requests for changes, faults and other modifications, we did not have access to a comprehensive list of them given the absence of a centralized registry. Based on the information obtained, we noted that productions were not always carried out in accordance with the best practices. For example, at the time of upgrading to version 5.1, the migration of the Kronos software package's components illustrates the testing process' shortcomings. In effect, this implementation had not been validated through functional tests, which would have made it possible—in this case—to confirm that the upgrade did not modify the processes. The implementation of this version caused errors in the calculation of time banks as at May 1, 2011 and ended up requiring a very substantial number of manual corrections.

Our audit of the tests conducted by the functional team for a few requests for changes confirmed that the validations are appropriate despite the fact that the strategy and scripts are still not very well documented. However, we must emphasize that it was not always possible to retrace the authorizations for the production and follow-up of certain changes. We must also emphasize that an individual acting independently from the development

² A test script is a detailed procedure for fully testing a function or an aspect of a function. The test plan describes *what* needs to be tested, whereas the test script describes *how* to conduct a particular test.

must handle the transfer of components in production but that the person in charge of the functional team is responsible for the final results and must approve all implementations.

We also wish to emphasize that several major IT changes were made after the Kronos software package had been implemented. These changes modified how the TM process operated. With respect to the best practices for a major IT project, it is recommended to have each component fully developed as close as possible to its final version before implementation in order to limit the changes to the production environment, since this practice increases risks considerably.

3.2.6.B. Recommendation

We recommend that the mandatory of the “time management” subproject, i.e., the Service des technologies de l’information, take the necessary measures to:

- develop a global strategy for carrying out tests as part of the implementation of the subsequent phases of the “time management” subproject;
- ensure that the test management tools are applied (test script template among others).

Business unit’s response:

[TRANSLATION] A global strategy will be developed for conducting tests, including follow-up.

*The strategy will be communicated to the principle stakeholders (**Planned completion: May 2013**)*

*The strategy, including follow-up testing, will be implemented when the project is transferred to the operational team. (**Planned completion: June 2013**)*

3.3. Security

3.3.1. Environment Management

3.3.1.A. Background and Findings

The architecture of the IT environments must separate functions from tasks to ensure data integrity and accuracy in each environment. The best IT environment management practices suggest creating different environments for specific objectives.

For the TM subproject, the STI implemented an environmental architecture that meets generally recognized standards and the need to segregate functions. The environments must be accessible to certain groups according to each group's roles and responsibilities, and the transfer of IT components must be controlled to ensure data accuracy and integrity. However, in fact, we noted that components were generally transferred between environments by the development personnel who had full control over them, including those of the production environment, without any control over accesses, follow-ups or tracking of the interventions carried out.

Moreover, the IT components must be developed, modified and tested in the development environment. They must then be transferred to the acceptance test environment as the project progresses. Once the acceptance tests have been approved, the components are transferred to the preproduction environment for compliance testing. Finally, once validated and approved by the expert users, the components must be transferred to the production environment.

To this end, we noted certain gaps in the management of these environments and transfers. IT components are transferred from the functional testing environment to the production environment without systematically passing through the preproduction environment and without any validation by the expert users. Although the STI now validates several of these components in the preproduction environment, the expert users are ultimately responsible for verifying changes and authorizing transfers, particularly in the production environment.

We also noted that the functional team is required to re-enter in the production environment specific parameters such as schedules because these parameters are not transferred to the production environment. This is not a recommended practice because not only does it require the duplicate entry of the parameters, but also these parameters are recorded and tested in the development environment, which increases the risk of errors. This task should be automated using tools such as Workforce Record Manager.

Moreover, the Kronos software package is installed in an environment based on the Windows Server operating system. The project team produces documents dealing with the architecture, and the Kronos user guides in these environments (e.g., development, production) are well documented.

This environment's security is managed—in accordance with the STI's practices—through policies and group strategies³ in the environment of the city's Service d'annuaire informatique. We noted that most of the controls were present and that the processes were generally documented. However, we also noted the lack of an audit strategy for these environments, specifically the production environment. Such a strategy would make it possible to keep traces of risky interventions carried out on TM data or related information.

3.3.1.B. Recommendation

We recommend that the Service des technologies de l'information take the necessary measures to:

- **control transfers of IT components between the environments;**
- **implement the necessary tools to ensure data integrity during IT component transfers between the environments.**

Business unit's response:

[TRANSLATION] At present, risk is managed by an internal procedure of the project team. The person (consultant) who transfers program components to the production environment is not the same person who developed them; this was done by a programmer analyst. A transfer document is systematically developed, updated and archived.

*Recognizing the problem, we developed and implemented a new acceptance environment. **(Completed, April 2013)***

We are in the process of developing a procedure to ensure that all development and parameterization is systematically followed by mandatory transfer to an acceptance environment.

To achieve this, the acceptance procedure that takes place in the functional team's environment will have to be reintegrated into the new environment. In this way, the acceptance process will be independent from development.

*We are also currently developing a procedure to set up Workforce Record Manager, which will be used for transfers to the production environment when the project is transferred to the operational team. **(Planned completion: June 2013)***

³ The "group strategies" (or GPOs [Group Policy Objects]) are centralized management functions available under the Microsoft Windows family. These functions are used to manage workstations and users in an Active Directory environment.

3.3.1.C. Recommendation

We recommend that the Service des finances, which owns the process, in collaboration with the Service des technologies de l'information, as part of the "time management" subproject, determine the potential risks in order to design and implement an audit strategy accordingly.

Business unit's response:

[TRANSLATION] Determine potential risks and implement an audit strategy. (Planned completion: December 2013)

3.3.2. Access Management

3.3.2.A. Background and Findings

Two main strategies can be used to configure access security in the Kronos software package. The first involves using the package's access management and access parameters to create an "owner"-type security. The Kronos software package was implemented with an owner-type security structure that is therefore subject to the package's configuration. The second strategy provides control using a gateway based on the LDAP⁴ which the city already uses. This strategy offers several advantages, the most important being the consolidation of user information in a single registry for several systems. However, it requires that all resources be identified in the directory. During our audit, the person responsible for this activity tested the LDAP-based approach with a target group to assess the possibility of implementing this strategy for all users. However, there were no orientations or directives provided for the implementation of this strategy in the case of the Kronos software package.

Application security in the Kronos software package was designed by the TM subproject's functional team by adapting the system's basic roles and responsibilities with respect to the city's situation in order to determine access profiles. Documents on the TM subproject management provided for the possibility of assigning up to 28 different access profiles to users, but the functional team reduced this number to 19, some of which are specific and temporary during the implementation of the Kronos software package.

We noted that the functional team ensures regular follow-up of the most critical profiles. However, we also noted certain situations where the best practices were not applied.

⁴ Lightweight Directory Access Protocol. Originally, the LDAP was a protocol used to query and modify directory services.

Indeed, the best practices recommend that high-privilege codes and profiles giving access to production environment data be assigned only to a limited number of users, that interventions using these codes be recorded in a restricted-access file and that the personnel use these privileges only as necessary to ensure data integrity, security and accuracy. The “SuperAccess” access profile that was configured in the Kronos software package authorizes unrestricted write access on all work attendance data. As with other user codes, actions leave traces, but these traces can also be modified or destroyed. We noted that this profile was assigned to seven users: four among the IT personnel and three in the functional team. In the case of this project, the number of users who have a privileged access profile appears high to us. Furthermore, the interventions made with this access profile are not documented and do not always leave traces—thus making it difficult to evaluate its relevance.

The owner-type approach has impacts on security management. Under this approach, a user may have several user codes with different access rights (profiles) since codes are managed and named manually without being directly validated by the city’s environment. The persons responsible for security management in the Kronos project standardized the user code format by aligning it with the city’s standardized user code nomenclature. However, four members of the STI’s implementation team also have another generic “administrator” user code with a “SuperAccess” profile. This is contrary to the best practices that proscribe the use of generic codes.

3.3.2.B. Recommendation

We recommend that the Service des finances, which owns the process, in collaboration with the Service des technologies de l’information, as part of the “time management” subproject and once the deployment has been completed (post-implementation):

- **review and justify the assignment of the “SuperAccess” profile to certain users while giving consideration to the available controls;**
- **validate the existing profiles and deactivate or destroy all access profiles that are not used or required;**
- **prepare an action plan and an implementation schedule for using the Lightweight Directory Access Protocol directory to control access to the Kronos software package.**

Business unit’s response:

[TRANSLATION] The review of access and security profiles, as well as of the assignment of the “SuperAccess” profile, is under way. Security profiles and access

to Kronos will be controlled and monitored in accordance with the recommendations contained in the report of the Bureau du vérificateur général on the protection of personal information. (Planned completion: June 2013)

3.3.3. Certification Deliverables

3.3.3.A. Background and Findings

In accordance with the city's applicable security frameworks, a software package that supports a business process such as TM must be independently certified by the STI's Information security and best practices section.

At the time of our audit, we noted that the certification deliverables inherent to the Kronos software package had not been obtained for the version in production. Although these deliverables had been completed in 2008, the scope of the Kronos package deployment had been considerably widened since that time and several changes had been made to the package. Under the circumstances and considering the very nature of the Kronos software package, in our opinion, it is imperative to update the security certification deliverables. To this effect, we must emphasize the importance of protecting the ownership of the software package in trust, which had not been done initially.

It is important to note that, in accordance with the frameworks, the project leader is required to control the filing of all deliverables and ensure that the security certifications of all new software packages installed in the city's environments have been filed.

3.3.3.B. Recommendation

We recommend that the Service des finances, which owns the process, take all necessary measures to obtain the required deliverables for the Kronos software package's security certification.

Business unit's response:

[TRANSLATION] Certification is under way. The report has been prepared and is in the acceptance phase with the Service des finances. (Completed, April 2013)

3.4. Performance

3.4.A. Background and Findings

The Kronos software package experienced major performance problems during phase 2, following its implementation in the boroughs and central departments. Version 5.1 of the

software package was implemented by the STI but its deployment was compromised by performance issues. To determine the root causes of the problem and find solutions, the city requested the help of a Kronos specialist to carry out a technical study titled “Workforce Central Data Analysis & Empirical Sizing”.

The data analysis conducted as part of this study did not detect any specific problem but suggested several improvements. Finally, and according to the STI, migrating the Kronos package from version 5.1 to version 6.1 as well as increasing the servers’ data processing capabilities solved the system performance problem. We also noted that certain improvements were made, including with load balancing and hyperfind query processing.

However, several users we consulted pointed out to us that they still experience slowdowns and performance issues with the Kronos software package, specifically during payroll closure periods. Since no new performance data were available, we asked the project team—which supervises the performance of the database and Web servers—if problems had been experienced. According to the team’s evaluations, the Kronos software package is not plagued by performance problems despite what users perceive. However, these evaluations are based only on the number of database prompts whereas other factors may have caused the performance problems.

Given that the number of users integrated in the software package increased substantially, the increased use of the hyperfind function and the comments made by the users we questioned, it would be relevant to analyse and track the system’s performance based on other metrics. It is important to note that the study pointed out potential problems with using the hyperfind function among other things. This function is used to enable wide-ranging queries throughout the database and operates by extracting a “view”⁵ that recalls several data structures in memory. Each hyperfind query can recall data from several database tables to provide the necessary information to answer the query. The processing of the query may be slowed down if many users call up this function concurrently.

⁵ A view is a virtual table, i.e., it refers to the data that are not stored in a database table and in which data originating from several tables can be consolidated.

3.4.B. Recommendation

We recommend that the Service des finances, which owns the process, in collaboration with the Service des technologies de l'information, as part of the "time management" subproject:

- determine the norms and standards that would be acceptable with respect to response times in different Kronos software package use situations;
- implement performance indicator tracking measures for all Kronos software package components;
- assess the need to oversee the hyperfind queries to reduce the load on the Kronos software package and improve its performance levels;
- evaluate the possibility of creating a data warehouse for time management and human resources data to reduce the load on the system during queries.

Business unit's response:

[TRANSLATION] Actions to be taken:

- Determine norms and standards;
- Implement indicator tracking measures;
- Oversee hyperfind queries in order to increase effectiveness and efficiency;
- Assess the possibility of creating a data warehouse for Kronos.

These actions will be taken in collaboration with STI's Section informatique. (Planned completion: December 2013)

3.5. Evolution of the Kronos Platform

3.5.A. Background and Findings

The recognized IT management reference frameworks state the importance of implementing an ongoing support, change management or improvement process for existing IT platforms. To this effect, the ITIL⁶ reference framework quotes a study conducted by IBM, which found that:

- 80% of incidents are detected by users;
- poorly controlled changes are responsible for 85% of incidents;
- users inevitably end up forming the testing team in lieu of the information technology unit;
- such a situation leads to a loss of operational efficiency and higher costs for the organization.

⁶ Information Technology Infrastructure Library.

We noted planning deficiencies with respect to the implementation of a management and evolution process for the new Kronos software package upon completion of the TM subproject. Such a process and the assignment of sufficient resources are essential to ensure the efficient operation of the TM system on an ongoing basis and more particularly at the time the software package or its database is updated or migrated. The resources assigned to this process may carry out the required changes in a secure and controlled change management environment and thus ensure the uniformity and compliance of processes and data after the completion of the project.

The lack of a management and evolution process could have caused among other things non-compliant changes stemming from a lack of expertise, database irregularities or inconsistencies and system interruptions. Consequently, correcting the situation could be very costly.

3.5.B. Recommendation

We recommend that the Service des finances, which owns the process, in collaboration with the Service des technologies de l'information, take the necessary measures to implement an ongoing support and evolution process for the Kronos software package.

Business unit's response:

[TRANSLATION] Processes and activities regarding payroll operations are already in place for the support and evolution of the IBM and Oracle systems. In June 2013, STI's Section informatique will add Kronos to the portfolio of software requiring ongoing support and evolution. (Planned completion: June 2013)

3.6. Continuity Plan

3.6.A. Background and Findings

The organization's continuity plan records all risks and afferent impacts and should include availability and continuity plans that are specific to each applicative system operated by the organization. This plan should be used as a tool for determining the securement strategy required to counter or mitigate the consequences of the event represented by a risk. The securement strategy involves the use of the necessary preventive and curative measures as well as the participation of several departments to ensure service continuity.

The TM system (Kronos) operates 24 hours a day, 7 days a week. It drives the payroll system—considered critical. Consequently, the TM system must also be considered a

critical system. We must emphasize that updating the cumulative time and time bank data for the purpose of closing payroll according to a specific frequency leaves little time for preparing the payroll. This situation is conducive to increasing risk levels. Currently, the Section sécurité de l'information et meilleures pratiques evaluates the criticality and assigns up to 24 hours of tolerance following an interruption of the TM system regardless of the particular date or period.

System availability is ensured using several measures, devices or other means designed to provide a certain level of robustness for time clocks, the system's applicative component and its database. According to the different STI units that manage components that are critical to system operations, in principle, a component may be recovered within a rather short period of less than five hours or within 24 hours in the case of major problems. However, we must emphasize that this assertion was never validated as part of a simulated recovery.

In an extreme situation assuming the unavailability of time data, one of the contemplated possibilities suggests processing payroll on the basis of a previous pay period and then making corrections. However, the efforts or repercussions involved in such a strategy have not been evaluated.

The STI also pointed out to us that five applicative servers are currently available in load balancing mode. The servers are housed in two different locations and the interruption of one server would not lead to the interruption of basic services to the users. However, the fact that an important application called "Connect" is installed on only one of the servers is a weak point. This could cause TM service recovery delays.

Despite all of the redundancy and continuity recovery means that were implemented, we note that the absence of an overall plan and appropriate documents coupled with the lack of certain key resources could increase delays and lead to problems, mainly during the payroll closing period when the time constraints are very tight.

3.6.B. Recommendation

We recommend that the Service des finances, which owns the process, in collaboration with the Service des technologies de l'information, as part of the "time management" subproject:

- determine a formal continuity plan that is both concerted and efficient;
- conduct periodic continuity tests to validate the necessary system recovery time and detect gaps that need to be corrected, including adding the "Connect" component to the other servers.

Business unit's response:

[TRANSLATION] Development and implementation of an efficient continuity plan in collaboration with the STI. (Planned completion: June 2013)