Office of the Auditor General

AUDIT OF THE IT PROCESSES OF THE COMPUTERIZED FINANCIAL SYSTEM

2006 Report

Chapter 6

Table of Contents

EXECUTIVE SUMMARY

Introduction

The Audit of the IT Processes of the Computerized Financial System (SAP) was part of the 2006 Audit Plan brought forward by the City's Auditor General and received by Council on December 15, 2004.

Since amalgamation, all City of Ottawa departments have had to adopt new business practices. Audits conducted over the past two years, such as the Audit of the Management Control Framework and the Management Letters given to the City of Ottawa subsequently to their fiscal 2003, 2004 and 2005 year-end financial statement audits, have highlighted the need for a detailed review of the City of Ottawa's IT Processes of the Computerized Financial System.

Background

- In 1999, two years prior to the City's amalgamation, the Regional Municipality of Ottawa-Carleton completed an $11 million implementation of SAP to replace non-Y2K compliant legacy systems used for financial management, procurement, maintenance management and transit vehicle maintenance functions at the Region.
- In 2000, the Transition Board identified SAP as the new City of Ottawa's Enterprise Resource Planning (ERP) system.
- To consolidate municipal legacy systems, the Integrated Business Solutions (IBS) program was initiated. This program consisted of two capital projects:
    1. IBS Phase 1 (2001) addressed the consolidation of 12 different municipal financial and procurement systems at a cost of $5.3 million; and
    2. IBS Phase 2 (2004) consolidated 8 Human Resource systems, implemented an entirely new application for the City's corporate landlord function and consolidated various maintenance management systems into SAP at a cost of $39.2 million.
- The SAP environment is currently supporting the financial reporting process and multiple sub-systems, including the revenue and disbursements cycles.
- In November 2006, there were approximately 8,750 active users of the system, with approximately 7,400 being Employee Self Service users, which allows them, among other things, to manage their personal human resources records.
- The SAP Support Centre has an operating budget of $5.3 million to cover compensation costs of $3.1 million, and service purchase costs of $2.2 million of which $1.5 million is for SAP annual maintenance, which consists primarily of license costs. There are 32 full-time equivalent (FTE) staff positions in the SAP

Support Centre Unit and approximately 365 FTE staff positions, in Information Technology Services Branch.

- The recent large-scale SAP initiative is the SAP Platform Sustainment Program; with a work plan that included management reporting, bar coding, and other enhancements at a cost of $17.7 million (as of May 2006).
- The total up-to-date implementation cost is $73.2 million, not including the latest deployment of the SAP Human Resources module.
- The most recent SAP initiative was the deployment of the SAP Human Resources module, which provided access to all employees to manage their personal information file.

Audit objectives

The objectives of this audit were to provide an independent and objective insight into:

- The effectiveness of the IT general controls surrounding the SAP environment;
- The current state of SAP security; and
- The appropriateness of specific SAP-based documentation.

Audit Scope

The scope of the project was restricted to the following processes relevant to the live SAP production environment:

IT General Controls Supporting the SAP Environment

The criteria used were as follows:

- Are there well designed and operating program change controls;
- Are there well designed and operating logical access management controls; and
- Are there well designed and operating operations controls.

In testing the IT general controls supporting the live production SAP environment, we applied a statistical sampling approach to obtain a selection of representative samples. We utilized a statistical method based on the expectation of finding few or no errors. As a result, based on Poisson-based audit risk tables, we applied the lower of 25 or 10% of the population rule.

SAP Security

The criteria used were as follows:

- Appropriateness of logical access to BASIS[1] sensitive transactions;
- Appropriateness of SAP application layer security parameters;
- Assessment of "Super-user" existence; and
- Assessment of additional key risk areas.

SAP-Based Documentation

The criteria used were as follows:

- Appropriateness of documented IT General Controls support documentation;
- Appropriateness of user support documentation; and
- Appropriateness of logical access support documentation.

Key findings and Recommendations

1. IT General Controls

The existing IT general controls, while well designed, lack consistent evidence to determine whether they are operating effectively.

Specifically, we noted that there appears to be occasional lack of adherence to the formally documented internal control activities associated with the logical access[2] and program change management[3] processes. These results indicate an apparent lack of adherence to documented internal requirements and generally accepted sound IT control practices.

The existing control environment is highly supported by manual controls, versus automated SAP controls. Consequently, as consideration is given to increasing to a more appropriate automated control level, improvement must occur at the IT general control levels since it is these controls which lay the foundation for the continued effective and authorized operation of the SAP application.

[1] BASIS is the SAP term equivalent to a system administrator; who has very powerful accesses.

[2] Logical access processes include the creation of new users within SAP, changing user accesses to existing users as well as removing departed/terminated users on a timely basis.

[3] Program change management processes include proper approvals of program changes, appropriate testing prior to implementation in the live production environment, and a separation of duties between programmers and those individuals approving and promotion changes into the live production environment.

Recommendation 1

That Information Technology Services Branch ensure that:
(a) The control activities set out within the City of Ottawa policy documents be emphasised as required steps in all circumstances;

(b) The evidence of the performance of the prescribed control activities be retained for audit and monitoring purposes; and

(c) As it pertains to withdrawn/terminated users, more diligent application of logical access management policies as well as a more robust communication protocol between Employee Services Branch and Information Technology Services Branch be enforced to ensure timely reaction to access removal. Furthermore, routine (i.e. quarterly) review of employee lists, last logons, etc. would also greatly reduce the risks associated with having terminated users.

Management Response

1(a)/1(b): Management agrees with this recommendation. The Information Technology Services (ITS) Branch will continue to communicate the importance of following documented processes and retaining appropriate evidence, to staff, by means of email reminders, staff meetings, and employee performance evaluations.

1(c): Management agrees with this recommendation. On October 30th 2005, the City implemented an Enterprise Directory Services (EDS). EDS provides the information required to automate the locking of "terminated" employee Network and SAP applications accounts. It also automates the adjustment of SAP application privileges when employees move from one position to another. This has significantly improved the administration and timeliness of account administration.

2. SAP Security

We noted that sensitive access has been appropriately restricted and the highly complex production SAP environment is relatively securely configured.

However, we have observed that some key BASIS sensitive transactions are not appropriately limited to BASIS personnel, of which there should only be approximately four to five. Furthermore, there was one instance of an Information Technology Services Branch student[4] having highly privileged access.

BASIS objects are high risk because, in combination with certain transactions, they have the potential for the corruption or destruction of the SAP R/3 system or data.

[4] As was verbally represented to us when we inquired as to the identity of the user.

Additional emphasis should be placed on maintaining, and improving, the SAP security layer, since it plays a vital role to the continued operational effectiveness of SAP.

Recommendation 2

That Information Technology Services Branch, SAP Support Center Unit (SAP security group), in conjunction with senior management, using the information noted herein as well as the existing authorization audit reports:
(a) Execute a review of users with access to BASIS sensitive development activities, objects, transactions and Standard SAP BASIS profiles to ensure that high level access in SAP is restricted to users who require this level of access as part of their job;

(b) Remove access to the productions environment for all SAP ABAP developers;

(c) Place a particular emphasis on external consultants, who normally have privileged levels of access. Their accesses should be approved, well monitored and removed in a timely fashion; and

(d) Reconsider providing highly privileged access to SAP to a temporary Information Technology Services Branch student.

Management Response

2(a): ITS Branch currently conducts a monthly review of all sensitive user accounts and the assignment of sensitive privileges. ITS will investigate the impact of further access restrictions to sensitive BASIS roles. This will be initiated in Q2 of 2007.

2(b): Management disagrees with this recommendation. SAP ABAP Programmers require production access to investigate and diagnose production- related problems. SAP Production global system settings prevent programmers from altering programs or altering application configuration tables. These changes can only be created in the development environment and must follow the published approval process before being promoted to production. Adjustment of global system parameters is restricted, monitored and logged.

2(c): Management agrees with this recommendation. External consultants are not automatically provided production access. Production access is provided to consultants to allow them to perform their roles only after competence and performance is assessed. Consultant network accounts currently have end dates applied when created, this ensures that accounts are automatically locked by the EDS interface when contract end date are reached. This will be initiated in the second quarter of 2007.
2(d): Management agrees with this recommendation. It is not standard practice to provide student positions with privileged access. In the instance cited, the temporary student employee was granted the access after gaining four months of experience and being retained for a second work term. ITS will review authorization

assignments to determine if more restricted roles can be assigned. This will be initiated Q2 2007.

3. SAP-Based Documentation

We noted numerous instances of documentation which appears to be outdated or in draft format. As a result, there is a risk of inappropriate decision-making based on no longer, fully or partially, applicable documentation. In addition, if used for troubleshooting, maintenance or training purposes, there is an increased likelihood of lost time and effort due to the possible inaccuracy of some of the document contents. Finally, a lack of updated documentation or long-standing draft status may be an indicator of weaknesses in the overall internal control framework, which mandates the requirement for updating and formally approving policies, process descriptions, procedures and key support documents.

Furthermore, we reviewed documentation associated with the initial installation and configuration of SAP which assisted with the automation of certain control activities, or lack thereof. The documentation and the responses therein, demonstrate that there is a significant level of manual controls in place versus having preventive and detective controls with SAP. While the level of automated controls within a business process is highly dependent on the nature in which business is actually conducted; automated preventive controls are more sensitive and timely than manual controls. They support a more robust control environment and, when properly configured, reduce the likelihood of material errors, inappropriate transactions, the need for more time-consuming manual activities, etc.

Recommendation 14

That Information Technology Services Branch require that all relevant SAP-based documentation be:

- **Immediately updated;**
- **Routinely[5] updated;**
- **Formally approved and communicated, to represent the current state of each process; and**
- **Incorporated within the scope of their existing document management strategy, which has refresh and update requirements.**

[5] Generally accepted guidelines on regularity include a minimum of once a year assessment, or in conjunction with material environmental changes, for continued applicability. Furthermore, as part of any significant SAP project activity, there should be a required procedures/step to "Assess the impact of the project to existing documentation and updating thereof".

Management Response

Management agrees with this recommendation.

The ITS Branch recognizes the importance and necessity of maintaining current documentation. Workload demands, staff vacancies, and the volume of documentation dictate that different priorities are placed on different document types. System administration procedures and system configuration are given the highest priorities. The Branch will formally implement a document process for high priority documents to ensure they are approved, periodically reviewed and updated.

The ITS Branch identifies a requirement for a technical document writer to assist with document preparation and updating (140 days @ $600 per day – $84,000) to be initiated in Q3 2007 depending on resource availability.

In the case of business process documents, the ITS Branch relies on business process owners to vet all requested SAP change requests to ensure they comply with acceptable business practices and procedures. In the case of major changes or addition of controls, business acceptance testing is also performed.

4. Recommendations Arising from the Detailed Report

The following provides a summary of the specific recommendations as well as management responses resulting from the detailed audit work. The full discussions relating to these can be found in the detailed audit report, Section - Detailed Findings and Recommendations.

4.1 Dormant Users

Recommendation 3

(a) That Information Technology Services Branch review, the users who are inactive, have never logged on or work on a seasonal schedule with a particular and immediate focus on excluding those users who only have SAP access due to the SAP ESS/HR functionality granted to all employees.

(b) That Information Technology Services Branch remove/restrict/disable accounts that are no longer required on a regular basis (i.e. quarterly).

(c) That Information Technology Services Branch determine the true usage rates of SAP to provide context for any more stringent access controls and possible user account removal.

Management Response

3(a): Management agrees with this recommendation.

Non-ESS/MSS accounts are reviewed regularly because of the costs associated with the licensing. ITS will include Employee Self Service accounts in the nightly process, which automatically locks accounts dormant for more than 60 days. This will be initiated in Q2 2007.

The ITS Branch in conjunction with Employee Services Branch will review the number of re-activation requests in Q4Q4 2007 to determine if the development of a self-serve account re-activation function is warranted. Should the re-activation function be required, the Branch estimates 20 days of effort ($20,000 of consultant services) to be initiated in Q1 2008.

The Employee Services Branch has also identified several initiatives in their Q3 2007 work plan designed to increase the usage of ESS. These initiatives include updating current content and reports to make the site more user friendly as well as undertaking a promotion campaign focusing on the usability and convenience of the site.

3(b): Management agrees with this recommendation and it has already been implemented. With the implementation of the Enterprise Directory Services (EDS) in October 2005, all SAP accounts are automatically reviewed daily with current SAP HR employee status information. SAP user accounts are automatically locked upon employee termination and access privileges are adjusted based on the position that the employee occupies. In addition to the implementation of EDS, ITS uses an SAP password generation utility to assign a system generated initial password. Users are notified of the initial password by email or by phone and must login and change password within 24 hours or the account is automatically locked. In the case of ESS accounts, system generated passwords are generated and stored in SAP. These account passwords are never published. ESS user authentication is based on Microsoft's active directory single sign-on utilizing the user's network account

3(c): Recommendation requires the implementation of recommendation 4B. After profile usage logging has been implemented, the Branch will generate new usage rates based on log information in Q2 of 2008.

4.2 SAP System Parameters

Recommendation 4

That Information Technology Services Branch enable SAP auditing as per generally accepted practice to allow for the auditing of key activities within SAP. In conjunction with the enablement, IT and business management should define the key events they wish to audit and on what frequency while balancing the need for timeliness of review. Similarly, these events should be regularly assessed for continued applicability.

Management Response

ITS Branch, in partnership with the affected business process owners (e.g. Financial Services, Employee Services, and Surface Operations Branch, etc.), will conduct an assessment of the impact of implementing audit logging in Q3 2007.

Implementation will begin in Q1 2008 depending on requirements and resource availability identified in the assessment phase. The assessment will begin in Q3 of 2007. The initial high-level assessment for the implementation is identified as approximately: 20 days audit consultant $45,000; 10 days Basis $10,000; and 30 days business staff $10,000.

4.3 SAP Standard BASIS Profiles

Recommendation 5

(a) That Information Technology Services Branch immediately review the users and generic user ids with access to SAP Standard BASIS profiles S_A.CUSTOMIZ; S_A.DEVELOP; S_A.SYSTEM; and SAP_NEW for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(b) That Information Technology Services Branch consider establishing monitoring controls for when the profiles are actually utilized.

Management Response

5(a): Management agrees with this recommendation. The Branch will complete a review of Userids with access to SAP Basis roles to reduce the total number of assignments in Q2 2007.

5(b): The Branch will implement quarterly monitoring controls of profile usage. This recommendation is dependant on the implementation of audit recommendation 4B scheduled for Q2 2008.

4.4 Development Activities

Recommendation 6

(a) That Information Technology Services Branch restrict or provide at display-only access in production, to Data Dictionary Maintenance (SE11) and Program Maintenance (SE38) transactions. Any changes should be made in the development environment, be properly tested, and then transported to production.

(b) That Information Technology Services Branch immediately review the users and generic user ids with access to Data Dictionary Maintenance (SE11) and Program Maintenance (SE38) for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(c) That Information Technology Services Branch limit access to the Data Dictionary Maintenance (SE11) transactions to database administrators and implement mitigating controls to ensure these types of changes are not occurring in the production environment without proper approval.

Management Response

Management agrees with this recommendation. At the beginning of 2006, the ITS Branch implemented a granting approval process for several sensitive transactions including SE11 and SE38 in production. Access is granted for a specific duration and only with Support Centre project manager approval. SAP Production global system settings prevent any program maintenance access. Program changes can only be created in the development environment and must follow the published approval process before being promoted to production. Adjustment of global system parameters is restricted, monitored and logged.

4.5 Transport Administration Access

Recommendation 7

(a) That Information Technology Services Branch immediately review the users and generic user ids with access to impact the transport system through SE01, SE06, SE10 and STMS transactions for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(b) That Information Technology Services Branch restrict access to a limited number of BASIS users.

Management Response

7(a): Management agrees with this recommendation. ITS Branch will review Userids with access to SE01, SE06, SE10 and STMS transactions for reasonableness in Q2 2007.

7(b): Management agrees with this recommendation. The ITS Branch will restrict transactions to a limited number of users, however these will not necessarily be limited to BASIS accounts only. This action will be initiated Q2 2007.

4.6 SAP BASIS Sensitive Objects[6]

4.6.1 Role Administration (S_USER_AGR)

Recommendation 8

That Information Technology Services Branch review the users and generic user ids with access to object S_USER_AGR for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits to ensure appropriate segregation of duties are maintained.

Management Response

Management agrees with this recommendation. This action will be initiated in Q2 of 2007.

4.6.2 Displaying or Maintaining Source Code (S_DEVELOP)

Recommendation 9

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_DEVELOP for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

The ITS branch will initiate this recommendation in Q2 2007.

4.6.3 Transport Management (S_TRANSPRT)

Recommendation 10

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_TRANSPRT for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. Information Technology Services Branch does not identify any new or additional cost and will be initiated second quarter 2007.

[6] SAP Authorization objects control what transactions and operations users can execute.

4.6.4 Administration of the Change and Transport System (S_CTS_ADMI)

Recommendation 11

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_CTS_ADMI for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This action will be initiated in Q2 of 2007.

4.6.5 Changing Client-Independent Tables (S_TABU_CLI)

Recommendation 12

That Information Technology Services Branch immediately review the users and generic users ids with access to object S_TABU_CLI for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This will be initiated in Q2 of 2007.

4.6.6 Controlling Table Displaying and Maintenance (S_TABU_DIS)

Recommendation 13

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_TABU_DIS for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This action will be initiated in the second quarter of 2007.

Conclusion

Controlling access to its information technology system(s) is a key component for any corporation to uphold a robust control environment. Successful internal controls must therefore start with management stringent access restriction and continuous review of its access administration framework for non-compliance and excessive access. In our opinion, the City may have a greater number of privilege users, than typically expected, posing a potential risk to the City's Corporate Financial Management System (SAP).

The existing IT general controls were found to be well designed. However, we found a lack of consistent internal control activities associated with the logical access and program change management process.

Clear and readily accessible documentation is indicative of sound internal controls. Although SAP-based documentation was available for review, these were found to be in long-standing draft form and therefore may no longer be valid and not reflect the current state of the system. Outdated documentation poses the unnecessary potential risk that changes or steps are no longer relevant or may no longer apply. Improvements are therefore immediately needed to clearly update Corporate Financial Management System (SAP) documentation and a process established to ensure its adequacy and continual review and update.

We believe that all recommendations contained in this report can be implemented without the requirement for additional funds. However, this may require strategic redeployment of existing resources, both dollars and persons.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by Management.

SOMMAIRE

Introduction

La vérification des opérations du système financier informatisé (SAP) reposant sur la technologie de l'information (TI) faisait partie du plan de vérification de 2006 préparé par le vérificateur général de la Ville et reçu par le Conseil municipal le 15 décembre 2004.

Depuis la fusion, tous les services de la Ville d'Ottawa ont dû adopter de nouvelles pratiques administratives. Les vérifications menées au cours des deux dernières années, comme la vérification du cadre de contrôle de gestion et les lettres de recommandations remises à la Ville après les vérifications des états financiers de fin d'exercice pour les années 2003, 2004 et 2005, ont attiré l'attention sur la nécessité de mener un examen détaillé des opérations du système financier informatisé (SAP) reposant sur la technologie de l'information (TI) de la Ville d'Ottawa.

Contexte

- En 1999, deux ans avant la fusion municipale, la Municipalité régionale d'Ottawa-Carleton avait achevé, au coût de 11 millions de dollars, la mise en œuvre du système SAP qui remplaçait le système existant jugé non conforme aux exigences de l'an 2000, alors utilisé pour la gestion financière, les marchés publics, la gestion de l'entretien et les fonctions d'entretien des véhicules de transport en commun de la Région.
- En 2000, le Conseil de transition a choisi SAP comme nouveau système de gestion intégrée des ressources (GIR) de la Ville d'Ottawa.
- Afin d'amalgamer les anciens systèmes municipaux, le programme Solutions commerciales intégrées (SCI) a été adopté, lequel comprenait deux projets d'immobilisations :

1. la phase 1 du SCI (2001) prévoyait l'harmonisation des systèmes financiers et d'approvisionnement de l'administration régionale et des 11 municipalités fusionnées, au coût de 5,3 millions de dollars;

2. la phase 2 du SCI (2004) consistait à fusionner huit systèmes de ressources humaines, à implanter une toute nouvelle application pour la fonction de bailleur de la Ville et à regrouper divers systèmes de gestion de l'entretien dans SAP, au coût de 39,2 millions de dollars.

- L'environnement SAP soutien actuellement le processus des rapports financiers et de multiples sous-systèmes, y compris les cycles de revenus et de décaissement.

- En novembre 2006, on comptait quelque 8 750 utilisateurs actifs du système, dont 7 400 environ utilisaient le site de libre-service destiné aux employés, leur permettant, entre autres, de gérer leur dossier personnel de ressources humaines.
- L'Unité du Centre de soutien au SAP dispose d'un budget de fonctionnement de 5,3 millions de dollars qui sert à financer les coûts de la rémunération établis à 3,1 millions de dollars et les coûts d'achat de service qui s'élèvent à 2,2 millions de dollars, dont 1,5 million sont consacrés à la maintenance annuelle de SAP, qui consiste principalement en droits d'utilisation. L'Unité du centre de soutien au SAP compte 32 postes équivalent temps plein (ETP) tandis que la Direction des services de la technologie de l'information englobent environ 365 postes ETP.
- La plus récente initiative SAP à grande échelle a été le Programme de viabilité de la plate-forme de SAP, dont le plan de travail comprenait la préparation des rapports de gestion, le codage par code à barres et d'autres améliorations évaluées à 17,7 millions de dollars (en date du mois de mai 2006).
- Le coût total de la mise en œuvre s'élève à ce jour à 73,2 millions de dollars, chiffre qui exclut le déploiement le plus récent du module de ressources humaines SAP.
- La plus récente initiative SAP a été le déploiement du module de ressources humaines SAP qui permet à tous les employés de gérer leur dossier de renseignements personnels.

Objectifs de la vérification

Cette vérification avait pour objectifs d'analyser de façon indépendante et objective les éléments suivants :

- l'efficacité des contrôles généraux de TI en ce qui a trait à l'environnement SAP;
- l'état actuel de la sécurité de SAP;
- la validité de la documentation rattachée spécifiquement à SAP.

Portée de la vérification

La portée du projet se limitait aux procédés suivants qui relèvent de l'environnement opérationnel de production SAP :

Contrôles informatiques généraux soutenant l'environnement SAP

Les critères suivants ont été utilisés :

- Les contrôles mis en place pour les modifications de programmes sont-ils bien conçus et opérationnels?
- Les contrôles appliqués à la gestion de l'accès logique sont-ils bien conçus et opérationnels?

- Les contrôles permettant de vérifier les opérations sont-ils bien conçus et opérationnels?

Pour les tests visant à vérifier les contrôles informatiques généraux soutenant l'environnement de production actif du SAP, nous avons utilisé la méthode de l'échantillonnage statistique afin d'obtenir des échantillons représentatifs. Nous avons utilisé une méthode statistique en tablant sur le fait que nous ne trouverions que peu ou pas d'erreurs. Par conséquent, en nous basant sur les tableaux de risque de non-détection externe fondés sur la loi de Poisson, nous avons appliqué la règle du moindre, soit 25 ou 10 p. 100 de la population.

Sécurité de SAP

Les critères suivants ont été utilisés :

- Validité de l'accès logique aux transactions de nature délicate réservées au BASIS[7];
- Pertinence des paramètres des couches de sécurité d'application SAP;
- Évaluation de l'existence des « superutilisateurs »;
- Évaluation des autres grands domaines clés à risque.

Documentation rattachée à SAP

Les critères suivants ont été utilisés :

- Pertinence de la documentation de soutien des contrôles généraux de TI documentés;
- Pertinence de la documentation d'assistance à l'utilisateur;
- Pertinence de la documentation de soutien à l'accès logique.

Constatations et recommandations clés

1. Contrôles généraux de TI

Les contrôles généraux de TI sont bien conçus mais il n'existe pas suffisamment d'éléments probants (de pièces justificatives à l'appui) pour en établir l'efficacité de façon systématique.

Plus précisément, nous avons noté que les activités de contrôle interne formellement consignées qui sont associées aux procédés d'accès logique[8] et de gestion des

[7] BASIS est le terme employé par SAP pour désigner un administrateur de système qui détient de vastes pouvoirs d'accès.

[8] Les procédés d'accès logique comprennent la création de nouveaux comptes d'utilisateur dans SAP, les changements de niveau d'accès pour les utilisateurs existants de même que la suppression en temps voulu des comptes des utilisateurs ayant quitté leur emploi ou ayant été licenciés.

modifications de programmes[9] ne semblent pas être suivies en tout temps. Ces résultats indiquent un manque apparent de respect des exigences internes documentées et des méthodes de contrôle informatique saines et généralement admises.

L'environnement de contrôle existant est soutenu principalement par des contrôles manuels plutôt que par des contrôles SAP informatisés. Par conséquent, alors que la Ville songe à passer à un niveau de contrôle informatisé plus poussé, il est impératif d'améliorer le niveau des contrôles informatiques généraux, puisque ce sont ces contrôles qui forment la base de l'exploitation efficiente et autorisée de l'application SAP.

Recommandation 1

Que la Direction des services de la technologie de l'information s'assure que :

(a) l'on insiste sur l'importance de respecter en tout temps les activités de contrôle énoncées dans les documents de politique de la Ville d'Ottawa;

(b) les pièces justificatives de l'exécution des activités de contrôle prescrites sont conservées à des fins de vérification et de suivi;

(c) dans le cas des usagers qui ont quitté leur emploi ou qui ont été licenciés, les politiques de gestion de l'accès logique sont appliquées de façon plus expéditive, et qu'un protocole de communication plus ferme entre la Direction des services aux employés et la Direction des services de la technologie de l'information est appliqué pour que cet accès soit annulé rapidement. En outre, un examen systématique (c.-à-d. trimestriel) des listes d'employés, de la dernière ouverture de session, etc., réduirait considérablement les risques associés aux utilisateurs ayant quitté leur emploi.

Réponse de la direction

1(a)/(b) : La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information continuera de rappeler aux employés, au moyen de rappels par courriel, de réunions de service et d'évaluations de rendement, qu'il est important de suivre les procédés énoncés et de conserver les pièces justificatives,

1(c) : La direction est d'accord avec cette recommandation. Le 30 octobre 2005, la Ville a mis en œuvre un répertoire municipal (RM). Le RM fournit les données qui permettent de verrouiller automatiquement les comptes de réseau et d'application

[9] Les procédés de gestion des modifications de programmes comprennent l'approbation par l'autorité compétente de toute modification aux programmes, des tests effectués en bonne et due forme avant toute mise en œuvre de ces modifications dans l'environnement de production opérationnel, et le partage des tâches entre les programmeurs et les personnes qui approuvent et favorisent les modifications dans l'environnement de production opérationnel.

SAP des employés ayant quitté leur emploi. Il rajuste également automatiquement les privilèges d'application SAP lorsque les employés sont mutés, ce qui a considérablement amélioré la gestion et la rapidité d'administration des comptes.

2. Sécurité de SAP

L'accès aux transactions de nature délicate est restreint comme il se doit et l'environnement de production SAP, qui est très complexe, est configuré de façon relativement sûre.

Toutefois, nous avons observé que certaines transactions clés de nature délicate réservées au BASIS ne sont pas limitées au personnel BASIS comme il se doit, c'est-à-dire à environ quatre ou cinq personnes. En outre, dans un cas, un étudiant[10] travaillant pour Services de la technologie de l'information bénéficiait d'un accès hautement privilégié.

Les objets BASIS posent un risque élevé car, associés à certaines transactions, ils peuvent corrompre ou détruire le système ou les données SAP R/3.

Il serait nécessaire d'insister davantage sur la maintenance et l'amélioration de la couche de sécurité de SAP puisqu'elle joue un rôle primordial dans l'efficacité opérationnelle durable de SAP.

Recommandation 2

Que l'Unité du centre de soutien au SAP (groupe de sécurité SAP) de la Direction des services de la technologie de l'information, en collaboration avec les cadres supérieurs, tienne compte des données que renferme le présent rapport ainsi que les rapports existants de vérification des autorisations pour :

(a) revoir la liste des utilisateurs ayant accès aux activités de développement BASIS de nature délicate, aux objets, aux transactions et aux profils normalisés SAP BASIS, afin de s'assurer que l'accès privilégié à SAP est réservé uniquement aux utilisateurs qui en ont besoin pour faire leur travail;

(b) empêcher tous les programmeurs du logiciel ABAP de SAP d'avoir accès à l'environnement de production;

(c) s'intéresser tout particulièrement aux experts-conseils externes, à qui on accorde normalement un niveau d'accès privilégié. Cet accès devrait être approuvé, suivi de près et annulé en temps voulu;

[10] Selon ce qui nous a été dit lorsque nous avons demandé l'identité de cet utilisateur.

(d) repenser le bien-fondé de donner un accès hautement privilégié à SAP à un étudiant travaillant temporairement pour Services de la technologie de l'information.

Réponse de la direction

2(a) : La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information (STI) effectue actuellement un examen mensuel de tous les comptes utilisateurs de nature délicate et de l'octroi des accès privilégiés. STI examinera les effets de plus amples restrictions sur les rôles BASIS névralgiques. Ce travail débutera au deuxième trimestre de 2007.

2(b) : La direction n'est pas d'accord avec cette recommandation. Les programmeurs ABAP de SAP ont besoin d'accéder à la production pour pouvoir examiner et diagnostiquer les problèmes liés à la production. Les paramètres globaux du système de production SAP empêchent les programmeurs de modifier les programmes ou les tableurs de configuration de l'application. Ces modifications ne peuvent intervenir que dans l'environnement de développement et doivent suivre la procédure d'approbation publiée avant de passer à la production. Les rajustements aux paramètres globaux du système sont restreints, surveillés et consignés.

2(c) : La direction est d'accord avec cette recommandation. Les experts-conseils externes n'obtiennent pas automatiquement un accès à la production. C'est uniquement une fois que leur compétence et leur rendement ont été évalués que cet accès leur est octroyé pour leur permettre d'accomplir leurs tâches. Une date d'échéance est dorénavant assortie aux comptes réseaux des experts-conseils au moment où ceux-ci sont créés, si bien que ces comptes sont automatiquement verrouillés par l'interface RM lorsque le contrat arrive à échéance. Cette mesure prendra effet au deuxième trimestre de 2007.

2(d) : La direction est d'accord avec cette recommandation. Les étudiants ne disposent pas normalement d'un accès privilégié. Dans le cas précité, cet accès avait été accordé à cet employé temporaire, un étudiant, alors qu'il avait déjà quatre mois d'expérience et qu'il effectuait un deuxième stage. La Direction des services de la technologie de l'information a l'intention de revoir ces autorisations afin de déterminer si de tels employés peuvent être affectés à des rôles plus restreints. Cette mesure prendra effet au deuxième trimestre de 2007.

3. Documentation rattachée à SAP

Nous avons relevé de nombreux cas où la documentation semble périmée ou exister sous forme d'ébauche. De mauvaises décisions sont donc susceptibles d'être prises sur la foi d'une documentation totalement ou partiellement désuète. En outre, si cette documentation est utilisée à des fins de dépannage, d'entretien ou de formation, l'inexactitude éventuelle du contenu des documents dans certains cas pourrait entraîner

une perte de temps et d'efforts. En dernier lieu, l'absence de documentation à jour ou l'utilisation de longue date de versions ébauches pourrait signaler la présence de lacunes dans le cadre général des contrôles internes, cadre qui exige que les politiques, descriptions de procédés, procédures et documents de soutien clés soient mis à jour et approuvés officiellement.

De plus, nous avons effectué un examen de la documentation associée à l'installation et à la configuration initiales de SAP, utilisée dans le cadre de l'automatisation de certaines activités de contrôle ou en l'absence de tels contrôles, le cas échéant. La documentation et les réponses qu'elle renferme montrent qu'il existe un nombre considérable de contrôles manuels plutôt que de contrôles de prévention et de détection déclenchés par SAP. Bien que le niveau de contrôle automatisé au sein d'une fonction administrative dépende largement de la nature des fonctions en question, les contrôles automatisés de prévention sont beaucoup plus sensibles et rapides que les contrôles manuels. Ils soutiennent un environnement de contrôle plus robuste et, lorsqu'ils sont configurés correctement, réduisent la probabilité d'erreurs importantes et de transactions irrégulières ainsi que la nécessité d'effectuer des activités manuelles plus lentes, etc.

Recommandation 14

Que la Direction des services de la technologie de l'information exige que toute documentation pertinente rattachée à SAP soit :

- **mise à jour immédiatement;**
- **mise à jour régulièrement**[11]**;**
- **approuvée et communiquée officiellement afin de représenter correctement l'état actuel de chaque procédé;**
- **intégrée dans la stratégie courante de gestion des documents qui comprend des exigences de réviser et de mettre à jour.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

La Direction des services de la technologie de l'information reconnaît qu'il est important et nécessaire d'avoir une documentation à jour. La charge de travail, les postes vacants et le volume de documentation font en sorte que différentes priorités sont associées à différents types de documents. La première priorité est accordée aux

[11] Les lignes directrices généralement admises sur la régularité comprennent au minimum une évaluation annuelle, ou une évaluation effectuée lorsque des changements importants sont apportés à l'environnement, pour en assurer l'applicabilité continue. En outre, toute activité importante de projet SAP devrait inclure un procédé ou une étape obligatoire visant à « évaluer l'incidence du projet sur la documentation existante et sa mise à jour ».

procédures d'administration du système et à la configuration du système. La Direction des services de la technologie de l'information instituera une marche à suivre en bonne et due forme pour les documents à priorité élevée afin de s'assurer qu'ils sont approuvés, revus et mis à jour en temps opportun.

La Direction des services de la technologie de l'information reconnaît qu'elle requiert les services d'un rédacteur technique pour l'aider à préparer et à mettre à jour des documents (140 jours @ 600 $ par jour – 84 000 $); cette mesure prendra effet au troisième trimestre de 2007, sous réserve de la disponibilité des ressources.

Pour ce qui est des documents traitant des procédures administratives, la Direction des services de la technologie de l'information s'en remet aux responsables des procédures administratives pour vérifier toutes les demandes de modification à SAP afin d'en assurer la conformité avec les pratiques et procédures administratives admises. Des tests de validation et d'acceptation sont également effectués en cas de changements ou d'ajouts importants.

4. Recommandations découlant du rapport détaillé

Le lecteur trouvera ci-dessous un résumé des recommandations spécifiques de même que les réponses de la direction découlant du travail de vérification détaillé. Les détails figurent dans le rapport de vérification à la section intitulée Constatations détaillées et recommandations.

4.1 Utilisateurs inactifs

Recommandation 3

(a) Que la Direction des services de la technologie de l'information examine le cas des utilisateurs inactifs, des utilisateurs n'ayant jamais ouvert une session ou des travailleurs saisonniers, en portant une attention particulière et immédiate à l'exclusion d'utilisateurs qui n'ont accès à SAP que pour accéder à la fonction ESS/HR de SAP accordée à tous les employés.

(b) Que la Direction des services de la technologie de l'information fasse en sorte que les comptes qui ne sont plus utilisés régulièrement (c.-à-d. trimestriellement) soient annulés, restreints ou désactivés.

(c) Que la Direction des services de la technologie de l'information calcule les taux réels d'utilisation de SAP pour placer en contexte l'imposition de contrôles d'accès plus stricts et l'annulation éventuelle de comptes d'utilisateurs.

Réponse de la direction

3(a) : La direction est d'accord avec cette recommandation. Les comptes qui ne sont pas des comptes LSE ou LSG sont revus régulièrement à cause des coûts associés aux droits d'utilisation. La Direction des services de la technologie de l'information

inclura les comptes ESS (Libre service des employés) dans les exécutions de nuit qui verrouillent automatiquement les comptes inactifs depuis plus de 60 jours. Cette mesure prendra effet au deuxième trimestre de 2007.

La Direction des services de la technologie de l'information, de pair avec la Direction des services aux employés, examinera le nombre de demandes de rétablissement de comptes pendant le quatrième trimestre de 2007 afin de déterminer s'il serait justifié de créer une fonction libre-service de rétablissement de compte, auquel cas la Direction des services de la technologie de l'information estime qu'il faudrait compter 20 jours de travail (20 000 $ en honoraires d'experts-conseils) pour que la fonction soit amorcée au cours du premier trimestre de 2008.

La Direction des services aux employés a aussi relevé dans son plan de travail du troisième trimestre de 2007 plusieurs initiatives conçues pour augmenter le taux d'usage du ESS. Parmi ces initiatives, citons la mise à jour du contenu et des rapports actuels pour rendre le site plus convivial et le lancement d'une campagne de promotion axée sur la facilité d'emploi et la commodité du site.

3(b) : La direction est d'accord avec cette recommandation. Depuis la création du répertoire municipal (RM) en octobre 2005, tous les comptes SAP sont automatiquement revus quotidiennement et comparés aux données SAP actuelles des RH sur le statut des employés. Le compte d'un utilisateur SAP est automatiquement verrouillé lorsque l'employé quitte son emploi et les privilèges d'accès sont rajustés selon le poste qu'occupe l'employé. En plus d'avoir mis en œuvre le RM, la Direction des services de la technologie de l'information se sert d'un utilitaire générateur de mots de passe pour attribuer un premier mot de passe généré par le système. Les utilisateurs reçoivent un avis par courriel ou par téléphone les informant de leur premier mot de passe. Ils doivent alors ouvrir une session et changer le mot de passe dans les 24 heures, faute de quoi le compte est automatiquement verrouillé. Dans le cas des comptes ESS, les mots de passe produits par le système sont générés et stockés dans SAP. Ces mots de passe de comptes ne sont jamais publiés. L'authentification des utilisateurs est fondée sur l'identification unique de l'*Active Directory* de Microsoft qui emploie le compte réseau de l'utilisateur.

3(c) : La direction est d'accord avec cette recommandation qui requiert la mise en œuvre de la recommandation 4b). Une fois que l'enregistrement de l'usage des profils aura été exécuté, la Direction des services de la technologie de l'information produira les nouveaux taux d'utilisation fondés sur les données contenues dans le registre pendant le deuxième trimestre de 2008.

4.2 Paramètres du système SAP

Recommandation 4

Que la Direction des services de la technologie de l'information active la vérification SAP selon les pratiques généralement admises afin de permettre la vérification d'activités clés dans SAP. Conjointement à cette mise en activité, les gestionnaires de TI et des opérations devraient définir les événements clés qu'ils désirent vérifier ainsi que l'intervalle désiré, tout en tenant compte de la nécessité d'effectuer cet examen en temps opportun. Dans le même ordre d'idées, ces événements devraient être évalués régulièrement afin d'en confirmer l'applicabilité.

Réponse de la direction

La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information, en partenariat avec les responsables des procédés administratifs (par ex. la Direction des services financiers, la Direction des services aux employés et la Direction des opérations de surface) évaluera l'incidence de la mise en œuvre de la liste de contrôle de vérification pendant le troisième trimestre de 2007.

Cette mise en œuvre commencera au premier trimestre de 2008, selon les besoins et la disponibilité des ressources recensées au cours de la phase d'évaluation. Son coût approximatif est le suivant : 20 jours de vérification par des experts-conseils - 45 000 $; 10 jours de BASIS - 10 000 $; 30 jours pour le personnel chargé des opérations - 10 000 $.

4.3 Profils BASIS normalisés de SAP

Recommandation 5

(a) Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs qui ont accès aux profils BASIS normalisés de SAP (S_A.CUSTOMIZ; S_A.DEVELOP; S_A.SYSTEM et SAP_NEW) pour déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

(b) Que la Direction des services de la technologie de l'information songe à l'établissement des contrôles de surveillance lorsque les profils sont utilisés.

Réponse de la direction

5(a) : La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information effectuera un examen des identificateurs d'utilisateurs qui ont accès aux rôles BASIS de SAP en vue de réduire le nombre total d'affectations.

5(b) : La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information instituera des contrôles trimestriels de surveillance de l'utilisation des profils. Cette recommandation dépendra de la mise en œuvre au deuxième trimestre de 2008 de la recommandation 4b).

4.4 Activités de développement

Recommandation 6

(a) Que la Direction des services de la technologie de l'information restreigne l'accès à l'environnement de production, ou accorde un accès affichage seulement, aux transactions Maintenance du dictionnaire de données (SE11) et Maintenance des programmes. Toute modification devrait être effectuée dans un environnement de développement, correctement testée et transférée ensuite à la production.

(b) Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à la Maintenance du dictionnaire de données (SE11) et à la Maintenance des programmes (SE38) pour déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

(c) Que la Direction des services de la technologie de l'information limite aux administrateurs de bases de données l'accès aux transactions Maintenance du dictionnaire de données (SE11) et qu'elle mettre en œuvre des mesures de contrôle atténuants pour s'assurer que ce type de modification n'est pas effectué dans l'environnement de production sans l'autorisation requise.

Réponse de la direction

La direction est d'accord avec cette recommandation. Au début de 2006, la Direction des services de la technologie de l'information a institué un procédé d'autorisation pour plusieurs transactions de nature délicate, y compris les SE11 et SE38 en production. L'accès y est octroyé pour une durée déterminée, et ce, uniquement avec l'approbation du gestionnaire de projet du Centre d'assistance. Les paramètres globaux du système de production SAP empêchent l'accès à la maintenance des programmes. Les modifications aux programmes ne peuvent intervenir que dans un environnement de développement et doivent suivre la procédure d'autorisation publiée avant de passer à la production. Le rajustement des paramètres globaux du système est restreint, surveillé et consigné.

4.5 Accès à l'administration des transports

Recommandation 7

(a) Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs dont l'accès pourrait se répercuter sur le système des transports en raison des transactions SE01, SE06, SE10 et STMS, afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

(b) Que la Direction des services de la technologie de l'information limite cet accès à un petit nombre d'utilisateurs BASIS.

Réponse de la direction

7(a) : La direction est d'accord avec cette recommandation. Pendant le deuxième trimestre de 2007, la Direction des services de la technologie de l'information effectuera un examen des identificateurs d'utilisateurs ayant accès aux transactions SE01, SE06, SE10 et STMS pour déterminer si un tel accès est raisonnable.

7(b) : La direction est d'accord avec cette recommandation. La Direction des services de la technologie de l'information limitera ce genre de transactions à un nombre restreint d'utilisateurs. Toutefois, l'accès ne sera pas accordé uniquement aux comptes BASIS. Cette mesure prendra effet au deuxième trimestre de 2007.

4.6 Objets sensibles BASIS de SAP[12]

4.6.1 Administration du rôle (S_USER_AGR)

Recommandation 8

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet S_USER_AGR afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes pour s'assurer que le partage des tâches est bien respecté.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

[12] Les objets d'autorisation SAP contrôlent la nature des transactions et opérations pouvant être exécutées par les utilisateurs.

4.6.2 Affichage ou maintenance du code source (S_DEVELOP)

Recommandation 9

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet S_DEVELOP afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

4.6.3 Gestion du transport (S_TRANSPRT)

Recommandation 10

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet S_TRANSPRT afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

4.6.4 Administration du système de changement et de transport (S_CTS_ADMI)

Recommandation 11

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet (S_CTS_ADMI) afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

4.6.5 Modification apportée aux tableaux non rattachés aux clients (S_TABU_CLI)

Recommandation 12

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet S_TABU_CLI afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

4.6.6 Contrôle de l'affichage et de la maintenance des tableaux (S_TABU_DIS)

Recommandation 13

Que la Direction des services de la technologie de l'information revoie immédiatement les utilisateurs et identificateurs génériques d'utilisateurs ayant accès à l'objet S_TABU_DIS afin de déterminer si cet accès est raisonnable, et qu'elle continue à surveiller systématiquement les niveaux d'accès au moyen des vérifications d'autorisation existantes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Cette mesure prendra effet au deuxième trimestre de 2007.

Conclusion

Contrôler l'accès aux systèmes de technologie de l'information constitue un élément clé pour tout organisme qui souhaite maintenir un environnement de contrôle solide. L'efficacité des contrôles internes passe par la restriction rigoureuse de l'accès accordé par la direction ainsi que par un examen constant du cadre d'administration de cet accès en vue de déceler toute anomalie ou tout abus. À notre avis, le nombre d'utilisateurs ayant un accès privilégié pourrait être supérieur à la norme, représentant un risque potentiel de compromettre le système de gestion financière (SAP) de la Ville.

À notre avis, les contrôles généraux actuels de TI sont bien conçus. Toutefois, nous avons constaté une absence d'activités de contrôle internes concertées associées à l'accès logique et au processus de gestion des modifications aux programmes.

Une documentation claire et facilement accessible dénote la présence de contrôles internes solides. Bien que la documentation rattachée au SAP ait été mise à notre disposition pour examen, nous avons constaté que celle-ci existait sous forme d'ébauche

depuis longtemps. Il se peut donc qu'elle ne soit plus valide et qu'elle ne reflète plus l'état actuel du système. Une documentation périmée présente un risque potentiel inutile de changements ou d'étapes devenus superflus ou sans objet. Des améliorations immédiates s'imposent donc afin de mettre à jour la documentation du système de gestion financière (SAP) de la Ville et d'établir une procédure permettant de s'assurer que cette documentation est appropriée et qu'elle sera continuellement revue et mise à jour.

Nous croyons qu'il est possible de mettre en œuvre toutes les recommandations que renferme le présent rapport sans devoir engager de dépenses supplémentaires. Il se peut toutefois qu'un redéploiement stratégique des ressources humaines et financières soit nécessaire.

Remerciement

Nous tenons à remercier la direction de sa collaboration et de l'aide qu'elle a apportée à l'équipe de vérification.

1 INTRODUCTION

The Audit of the IT Processes of the Computerized Financial System (SAP) was part of the 2006 audit plan brought forward by the City's Auditor General and received by Council on December 15, 2004.

Since amalgamation, all City of Ottawa departments have had to adopt new business practices. Audits conducted over the past two years, such as the Audit of the Management Control Framework and the Management Letters given to the City of Ottawa subsequently to their fiscal 2003, 2004 and 2005 year-end financial statement audits, have highlighted the need for a detailed review of the City of Ottawa's IT Processes of the Computerized Financial System.

2 BACKGROUND

- In 1999, two years prior to the City's amalgamation, the Regional Municipality of Ottawa-Carleton completed an $11 million implementation of SAP to replace non-Y2K compliant legacy systems used for financial management, procurement, maintenance management and transit vehicle maintenance functions at the Region.
- In 2000, the Transition Board identified SAP as the new City of Ottawa's Enterprise Resource Planning (ERP) system.
- To consolidate municipal legacy systems, the Integrated Business Solutions (IBS) program was initiated. This program consisted of two capital projects:
  1. IBS Phase 1 (2001) addressed the consolidation of 12 different municipal financial and procurement systems at a cost of $5.3 million; and
  2. IBS Phase 2 (2004) consolidated 8 Human Resource systems, implemented an entirely new application for the City's corporate landlord function and consolidated various maintenance management systems into SAP for a cost of $39.2 million.
- The SAP environment is currently supporting the financial reporting process and multiple sub-systems, including the revenue and disbursements cycles.
- In November 2006, there were approximately 8,750 active users of the system, with approximately 7,400 being Employee Self Service users, which allow them, among other thing, to manage their personal human resources record.
- The SAP Support Centre has an operating budget of $5.3 million to cover compensation costs of $3.1 million, and service purchase costs of $2.2 million of which $1.5 million is for SAP annual maintenance, which consists primarily of license costs. There are 32 full-time equivalent (FTE) staff positions in the SAP Support Centre Unit and approximately 365 FTE staff positions, in Information

Technology Services Branch. The organizational chart of the Branch is presented below.

- The recent large-scale SAP initiative is the SAP Platform Sustainment Program; with a work plan that included management reporting, bar coding, and other enhancements at a cost of $17.7 million (as of May 2006).
- The total up-to-date implementation cost is $73.2 million, not including the latest deployment of the SAP Human Resources module.

The most recent SAP initiative was the deployment of the SAP Human Resources module, which provided access to all employees to manage their personal information file.

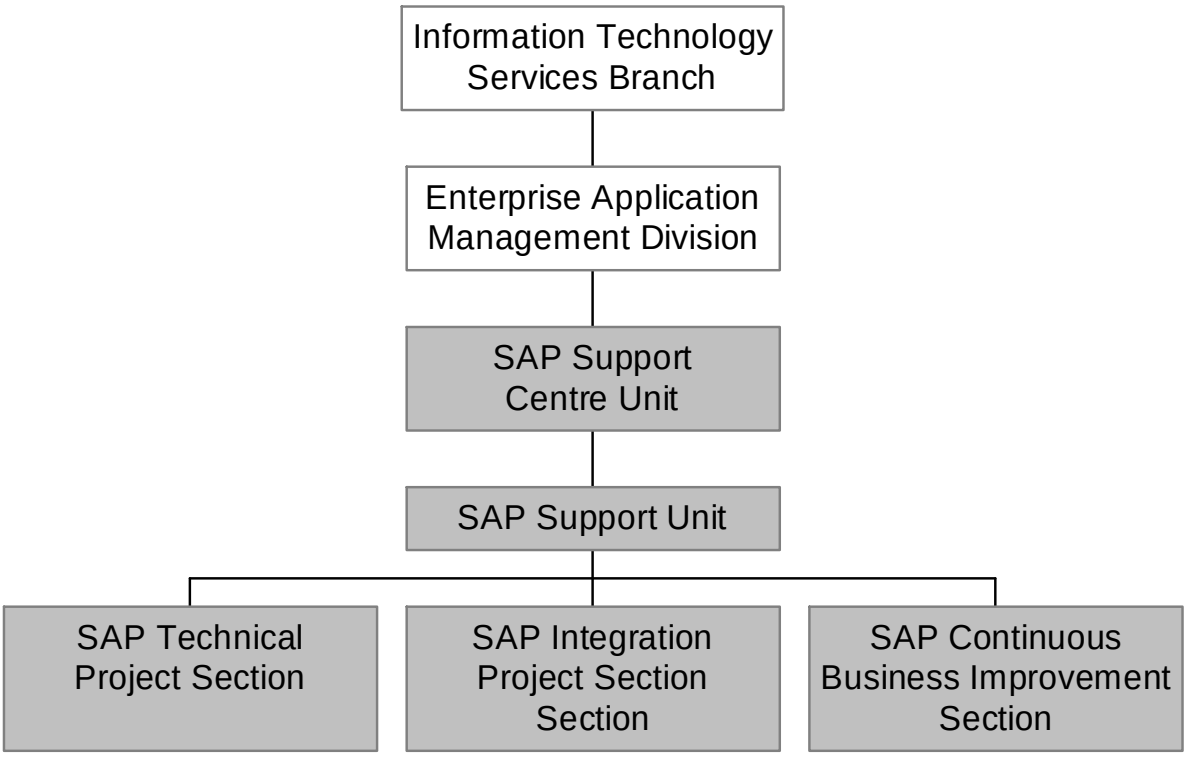

Figure 1: Organizational Chart - Information Technology Services Branch

3 AUDIT OBJECTIVES

The objectives of this audit were to provide an independent and objective insight into:

- The effectiveness of the IT general controls surrounding the SAP environment;
- The current state of SAP security; and
- The appropriateness of specific SAP-based documentation.

4 AUDIT SCOPE

The scope of the project was restricted to the following processes relevant to the live SAP production environment:

IT General Controls Supporting the SAP Environment

The criteria used were as follows:

- Are there well designed and operating program change controls;
- Are there well designed and operating logical access management controls; and
- Are there well designed and operating operations controls.

In testing the IT general controls supporting the live production SAP environment, we applied a statistical sampling approach to obtain a selection of representative samples. We utilized a statistical method based on the expectation of finding few or no errors. As a result, based on Poisson-based audit risk tables, we applied the lower of 25 or 10% of the population rule.

SAP Security

The criteria used were as follows:

- Appropriateness of logical access to BASIS[13] sensitive transactions;
- Appropriateness of SAP application layer security parameters;
- Assessment of "Super-user" existence; and
- Assessment of additional key risk areas.

[13] BASIS is the SAP term equivalent to a system administrator; who has very powerful accesses.

SAP-Based Documentation

The criteria used were as follows:

- Appropriateness of documented IT General Controls support documentation;
- Appropriateness of user support documentation; and
- Appropriateness of logical access support documentation.

5 DETAILED FINDINGS AND RECOMMENDATIONS

5.1 IT GENERAL CONTROLS

The existing IT general controls, while well designed, lacks the consistent evidence to determine whether they are operating effectively.

Specifically, we noted that there appears to be, as per the evidence reviewed, occasional lack of adherence to the formally documented internal control activities associated with the logical access[14] and program change management[15] processes.

From a logical access perspective, where there are 3 key control activities to be performed for each instance of a logical access event, within our 11 created-users sample there were 2 samples which were missing evidence of 1 key control being performed.

Similarly, approximately with our sample of 14 modified-users, there were 3 samples missing evidence of the initial manager approval (key control number one) and 5 samples missing evidence of a confirmation of the modification to the user profile (key control number three).

Finally, through some comparisons[16] of active user lists to departed/terminated employees lists, we identified 133 withdrawn/terminated employees who still had

[14] Logical access processes include the creation of new users within SAP, changing user accesses to existing users as well as removing departed/terminated users on a timely basis.

[15] Program change management processes include proper approvals of program changes, appropriate testing prior to implementation in the live production environment, and a separation of duties between programmers and those individuals approving and promotion changes into the live production environment.

[16] The specific procedures are detailed within our working papers and detail the specific steps taken to execute the testing.

access to the SAP system; based on the point in time file received for our review, which included seasonal employees who had retained their active status.

As a result of the identified weakness, there is an increased risk of inappropriate or unauthorised logical access, which can contribute to unauthorized transactions and segregation of duty conflicts.

From a program change perspective, approximately 10% of our 25-sample size had exceptions ranging from a lack of approved requests to lack of evidence of testing in a QA environment prior to production. More specifically, of the 5 key control activities which are to be performed for each program change, 4 samples were missing evidence of 1 key control being performed, 1 sample was missing evidence of 2 key controls being performed and 1 sample was missing evidence of 3 key controls being performed.

Consequently, there is an increased risk of unauthorized and inappropriate program changes, which can impact system integrity, internal control effectiveness, system performance and availability.

These results indicate an apparent lack of adherence to documented internal requirements and generally accepted sound IT control practices.

As was identified within the Audit of the Financial Control Environment report, the existing control environment is highly supported by manual controls (e.g., delegated signing authorities, contracting requirements for quotes), versus automated SAP controls. Consequently, as consideration is given to increasing to a more appropriate automated control level, improvement must occur at the IT general control levels since it is the IT general controls which lay the foundation for the continued effective and authorized operation of the SAP application.

Recommendation 1

That Information Technology Services Branch ensure that:

(a) The control activities set out within the City of Ottawa policy documents be emphasised as required steps in all circumstances;

(b) The evidence of the performance of the prescribed control activities be retained for audit and monitoring purposes; and

(c) As it pertains to withdrawn/terminated users, more diligent application of logical access management policies as well as a more robust communication protocol between Employee Services Branch and Information Technology Services Branch be enforced to ensure timely reaction to access removal. Furthermore, routine (i.e. quarterly) review of employee lists, last logons, etc. would also greatly reduce the risks associated with having terminated users.

Management Response

1(a)/1(b): Management agrees with this recommendation. The Information Technology Services (ITS) branch will continue to communicate the importance of following documented processes and retaining appropriate evidence, to staff, by means of email reminders, staff meetings, and employee performance evaluations.

1(c): Management agrees with this recommendation. On October 30th 2005, the City implemented an Enterprise Directory Services (EDS). EDS provides the information required to automate the locking of "terminated" employee Network and SAP applications accounts. It also automates the adjustment of SAP application privileges when employees move from one position to another. This has significantly improved the administration and timeliness of account administration.

5.2 SAP SECURITY

As part of our SAP security review, which was executed through the usage of complex SAP security analysis tools, we executed specified security review procedures around the production SAP application environment. Furthermore, we reviewed multiple examples of internal authorization audit reports, which demonstrate review of various SAP security components.

We noted that sensitive access has been appropriately restricted and the highly complex production SAP environment is relatively securely configured.

However, we have noted that some key BASIS sensitive transactions are not appropriately limited to BASIS personnel, of which there should only be approximately four to five. Furthermore, there was one instance of an Information Technology Services Branch student having highly privileged access.

BASIS objects are high risk because, in combination with certain transactions, they have the potential for the corruption or destruction of the SAP R/3 system or data. These high-risk objects should be allocated to security profiles. These profiles should be distributed to BASIS system administrators and a limited number of approved end-users, whose job function requires them to have access. Adequate restriction reduces the likelihood that errors or irregularities (intentional or unintentional) will occur.

Furthermore, in light of the observations in the previous point 1, regarding logical access shortcomings coupled with the segregation of duties comments raised within the Audit of the Financial Control Environment report, additional emphasis should be placed on maintaining, and improving, the SAP security layer, since it plays such a vital role to the continued operational effectiveness of SAP. Similarly, as was also highlighted within the Audit of the Financial Control Environment report, the existing

control environment is highly supported by manual controls, versus automated SAP controls. Therefore, as consideration is given to increasing to a more automated control level, continued improvement to the underlying SAP security layer must be jointly considered so as to ensure that those automated controls cannot be circumvented or "turned off".

Recommendation 2

That Information Technology Services Branch, SAP Support Center Unit (SAP security group), in conjunction with senior management, using the information noted herein as well as the existing authorization audit reports:

(a) Execute a review of users with access to BASIS sensitive development activities, objects, transactions and Standard SAP BASIS profiles to ensure that high level access in SAP is restricted to users who require this level of access as part of their job;

(b) Remove access to the productions environment for all SAP ABAP developers;

(c) Place a particular emphasis on external consultants, who normally have privileged levels of access. Their accesses should be approved, well monitored and removed in a timely fashion; and

(d) Reconsider providing highly privileged access to SAP to a temporary Information Technology Services Branch student.

Management Response

2(a): ITS Branch currently conducts a monthly review of all sensitive user accounts and the assignment of sensitive privileges. ITS will investigate the impact of further access restrictions to sensitive BASIS roles. This will be initiated in Q2 of 2007.

2(b): Management disagrees with this recommendation.

SAP ABAP Programmers require production access to investigate and diagnose production- related problems. SAP Production global system settings prevent programmers from altering programs or altering application configuration tables. These changes can only be created in the development environment and must follow the published approval process before being promoted to production. Adjustment of global system parameters is restricted, monitored and logged

2(c): Management agrees with this recommendation. External consultants are not automatically provided production access. Production access is provided to consultants to allow them to perform their roles only after competence and performance is assessed. Consultant network accounts currently have end dates applied when created, this ensures that accounts are automatically locked by the

EDS interface when contract end date are reached. This will be initiated in the second quarter of 2007.

2(d): Management agrees with this recommendation. It is not standard practice to provide student positions with privileged access. In the instance cited, the temporary student employee was granted the access after gaining four months of experience and being retained for a second work term. ITS will review authorization assignments to determine if more restricted roles can be assigned.
This will be initiated Q2 2007.

5.2.1 Dormant Users

The number of SAP users fluctuates throughout a year. At the time of our review in April 2006, there were 10,154 users.

During our dormant user review, which is based on reviewing all users and assessing when they last used the production SAP system, we identified the following issues:

- 1,727 users have not logged on in at least 90 days, representing approximately 17% of the total user accounts.
- 4,668 users who have never logged on to SAP, representing approximately 46% of the total SAP user accounts.
- 1,710 users have been locked due to administrator lock after periods of inactivity, representing approximately 17% of the total user accounts.

We appreciate that with the use of SAP HR all, or the majority of, employees have an SAP ID and, more often than not, this causes an overstatement of the aforementioned numbers. Furthermore, based on the data we obtained we could not assess which users only have SAP ESS (Employee Self-Service) - level access to manage their personal HR record. However, in April 2006, there were a total of 5,214 ESS users of which 3,254 had never logged on resulting in potential unnecessary license costs for the City.

Nevertheless, the figures clearly indicate the majority of users simply do not appear to require access.

Users who have not logged on over a large period of time may indicate transferred or terminated users. Given that the SAP accounts are still active for these users, until they are locked after 60 days, they can be accessed by other people (during that 60 day window) to execute unauthorized functions in SAP, especially if there has been a history of sharing passwords.

It should be noted that users who have never logged on would still have the default passwords assigned, which increases the risk of someone gaining unauthorized access to the account using commonly known passwords.

Finally, in order to lawfully create users within SAP, whether ultimately utilized or not, licenses fees are required to be paid to SAP. As a result, a focus should be made to ensure only those licenses, which really need to exist, are purchased. During our discussions, multiple users verbally indicated they have never used SAP, even for ESS purposes.

Recommendation 3

(a) That Information Technology Services Branch review, the users who are inactive, have never logged on or work on a seasonal schedule with a particular and immediate focus on excluding those users who only have SAP access due to the SAP ESS/HR functionality granted to all employees.

(b) That Information Technology Services Branch removed/restricted/disabled accounts that are no longer required on a regular basis (i.e. quarterly).

(c) That Information Technology Services Branch determine the true usage rates of SAP to provide context for any more stringent access controls and possible user account removal.

Management Response

3(a): Management agrees with this recommendation. Non-ESS/MSS accounts are reviewed regularly because of the costs associated with the licensing. ITS will include Employee Self Service accounts in the nightly process, which automatically locks accounts dormant for more than 60 days. This will be initiated in Q2 2007.

The ITS Branch in conjunction with Employee Services Branch will review the number of re-activation requests in Q4Q4 2007 to determine if the development of a self-serve account re-activation function is warranted. Should the re-activation function be required, the Branch estimates 20 days of effort ($20,000 of consultant services) to be initiated in Q1 2008.

The Employee Services Branch has also identified several initiatives in their Q3 2007 work plan designed to increase the usage of ESS. These initiatives include updating current content and reports to make the site more userfriendly as well as undertaking a promotion campaign focusing on the usability and convenience of the site.

3(b): Management agrees with this recommendation and it has already been implemented. With the implementation of the Enterprise Directory Services (EDS)

in October 2005, all SAP accounts are automatically reviewed daily with current SAP HR employee status information. SAP user accounts are automatically locked upon employee termination and access privileges are adjusted based on the position that the employee occupies. In addition to the implementation of EDS, ITS uses an SAP password generation utility to assign a system generated initial password. Users are notified of the initial password by email or by phone and must login and change password within 24 hours or the account is automatically locked. In the case of ESS accounts, system generated passwords are generated and stored in SAP. These account passwords are never published. ESS user authentication is based on Microsoft's active directory single sign-on utilizing the user's network account.

3(c): Management agrees with this recommendation. Recommendation requires the implementation of recommendation 4B. After profile usage logging has been implemented, the Branch will generate new usage rates based on log information in Q2 of 2008.

5.2.2 SAP System Parameters

During our review of SAP system parameter settings, which was part of overall SAP security review, we noted that a number of the security settings have not been configured in accordance to leading practice. Security related start-up parameters can be customized to control password requirements, user lock-out settings, time limits for sessions, logging of table changes, and other features. At present, the setting that controls how long a login password is valid is set to 60 days.

Of the multiple settings we assessed, we found that currently, the setting controlling SAP Auditing is not enabled, therefore, disabling the auditing feature.

Recommendation 4

That Information Technology Services Branch enable SAP auditing as per generally accepted practice to allow for the auditing of key activities within SAP. In conjunction with the enablement, IT and business management should define the key events they wish to audit and on what frequency while balancing the need for timeliness of review. Similarly, these events should be regularly assessed for continued applicability.

Management Response

Management agrees with this recommendation. ITS Branch, in partnership with the affected business process owners (e.g. Financial Services, Employee Services, and Surface Operations Branch, etc.), will conduct an assessment of the impact of implementing audit logging in Q3 2007. Implementation will begin in Q1 2008 depending on requirements and resource availability identified in the assessment

phase. The assessment will begin in Q3 of 2007. The initial high-level assessment for the implementation is identified as approximately:
20 days audit consultant $45,000; 10 days Basis $10,000; and 30 days business staff $10,000.

Generic User IDs:
We noted that the City has some generic user id's: DDIC and R3JOBS. There is a potential inherent risk that over time the password to a general account may become known to numerous users/administrators. Thereafter, anyone logging under the user ID have the capability of making any business transaction anonymously without an auditing trail to determine who conducted the activities.

User DDIC is a user with special privileges in installation, software logistics, and the ABAP Dictionary. It is used to change certain system parameters and maintains special privileges to software logistics and ABAP/4 dictionary. It is created during the installation of the R/3 System. Most of the time this ID can be accessed and consequently should be secured.

R3JOBS, Background Jobs usually represents a system account that manages JOBS (i.e. reports, interfaces, etc.). It can be a dialog user (User Type A) or Non Dialog user (User Type B) or even Communication user (User Type C). If type B or C the risk is low, if type A, then it should be secured.

During our review of profiles and transactions, which are further detailed in sections 2.3 to 2.6 inclusive, we determined that accesses to one or both of these generic user IDs are present in each object.

5.2.3 SAP Standard BASIS Profiles

SAP R/3 provides a wide array of "standard" BASIS profiles, which are tailored to different functions within a business. Within some key ones, there are inherent risks in using these in a production environment due to their powerful nature.

We identified nine users with access to these powerful profiles, which was greater than was our expectation. The main profiles where these users appeared include individual profiles which either:

- Contain all authorizations for BASIS activities in the Customizing menu (S_A.CUSTOMIZ);
- Represent a profile set up for developers working in the development environment (S_A.DEVELOP);
- Are for the System administrator (Superuser) (S_A.SYSTEM); and/or

- Contain unrestricted authorizations that are added since the previous SAP release (SAP_NEW).

Also included within the aforementioned profiles is SAP_ALL, which contains all authorizations for SAP and is consequently, an extremely powerful privilege to have.

The associated impact of possibly having too many users with access to these profiles is that they can technically impact system integrity, internal control effectiveness, system performance and availability. The greater the number of individuals with these accesses, the greater the risks.

These profiles should generally not be assigned to any end user and should be carefully monitored when used by any system or "firecall" ID.

Recommendation 5

(a) That Information Technology Services Branch immediately review the users and generic user ids with access to SAP Standard BASIS profiles S_A.CUSTOMIZ; S_A.DEVELOP; S_A.SYSTEM; and SAP_NEW for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(b) That Information Technology Services Branch consider establishing monitoring controls for when the profiles are actually utilized.

Management Response

5(a): Management agrees with this recommendation. The Branch will complete a review of Userids with access to SAP Basis roles to reduce the total number of assignments in Q2 2007.

5(b): Management agrees with this recommendation. The Branch will implement quarterly monitoring controls of profile usage. This recommendation is dependant on the implementation of audit recommendation 4B scheduled for Q2 2008.

5.2.4 Development Activities

Transactions allowing for Data Dictionary Maintenance (SE11) and Program Maintenance (SE38) allow the user to execute various development transactions. With these transactions, users may be able to run or edit programs (in SAP R/3 reports are programs and include those that delete master data and perform revaluation), make modifications or perform other development functionality, access the transport system, and display sensitive information bypassing proper procedure. This could impact the integrity and confidentiality of data, as well as the stability of the system.

We identified 11 users with access to Data Dictionary Maintenance (SE11) and 12 users to access to Program Maintenance (SE38), which was greater than was our expectation.

Recommendation 6

(a) That Information Technology Services Branch restrict or provide at display-only access in production, to Data Dictionary Maintenance (SE11) and Program Maintenance (SE38) transactions. Any changes should be made in the development environment, be properly tested, and then transported to production.

(b) That Information Technology Services Branch immediately review the users and generic user ids with access to Data Dictionary Maintenance (SE11) and Program Maintenance (SE38) for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(c) That Information Technology Services Branch limit access to the Data Dictionary Maintenance (SE11) transactions to database administrators and implement mitigating controls to ensure these types of changes are not occurring in the production environment without proper approval.

Management Response

Management agrees with this recommendation. At the beginning of 2006, the ITS Branch implemented a granting approval process for several sensitive transactions including SE11 and SE38 in production. Access is granted for a specific duration and only with Support Centre project manager approval. SAP Production global system settings prevent any program maintenance access. Program changes can only be created in the development environment and must follow the published approval process before being promoted to production. Adjustment of global system parameters is restricted, monitored and logged.

5.2.5 Transport Administration Access

Transport administration is the process of making changes to the production environment, which should be something very closely controlled and monitored. We identified 10 users with access to transactions allowing them to execute transactions impacting the transport system (CTS).

Users are allowed to perform activities to the correction and transport system through:

- Correction and transport system (SE01);
- System type table maintenance (SE06);
- Customizing organizer (SE10); and
- Transport management system (STMS).

With these accesses users may be able to perform unauthorized correction and transport system (CTS) activities bypassing proper procedures (e.g. program change management) and possibly impacting the integrity and stability of the SAP R/3 environment.

Access should be restricted to a limited number of BASIS users. These transactions should only be available on an as needed basis. Monitoring controls should be implemented to ensure the utilization of these types of transactions is closely monitored as well.

Recommendation 7

(a) That Information Technology Services Branch immediately review the users and generic user ids with access to impact the transport system through SE01, SE06, SE10 and STMS transactions for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

(b) That Information Technology Services Branch restrict access to a limited number of BASIS users.

Management Response

7(a): Management agrees with this recommendation. ITS Branch will review Userids with access to SE01, SE06, SE10 and STMS transactions for reasonableness in Q2 2007.

7(b): Management agrees with this recommendation. The ITS Branch will restrict transactions to a limited number of users, however these will not necessarily be limited to BASIS accounts only. This action will be initiated Q2 2007.

5.2.6 SAP BASIS Sensitive Objects [17]

Although access to the following objects is somewhat restricted at the transaction level, they should still be limited to key personnel who require this type of access. This will limit the risk of accessing critical transactions when adding them to non-restricted objects.

Role Administration (S_USER_AGR)

The SAP authorization object (S_USER_AGR), which allows a person to perform role administration (i.e., create, change, and delete roles) is very sensitive. Together with the other Sensitive BASIS objects, one can use this authorization object to distribute user administration, if different administrators are established to administer users. On its own this object allows no access to profiles or users, however, access to this object enables the creation and maintenance of security roles or activity groups and should be limited to those who are responsible for security.

[17] SAP Authorization objects control what transactions and operations users can execute.

We identified 36 users from both Financial Services Branch and Information Technology Services Branch with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object.

Security and BASIS administration functions should be segregated. The combination of these functions could result in undetected fraudulent activities.

Recommendation 8

That Information Technology Services Branch review the users and generic user ids with access to object S_USER_AGR for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits to ensure appropriate segregation of duties are maintained.

Management Response

Management agrees with this recommendation. This action will be initiated in Q2 of 2007.

Displaying or Maintaining Source Code (S_DEVELOP)

The SAP authorization object S_DEVELOP allows the user to display or maintain the source code for ABAP programs. Access to S_DEVELOP gives access to the screen painter (Dynpros – dynamic programs - are the input screens used for entering data), ABAP/4 development tools, ABAP/4 Dictionary and Data Modeller, Function Library, Object Browser, and Info System.

Some transactions requiring this object include:

- Data Dictionary Maintenance (SE11);
- Data Dictionary Display (SE12);
- Maintain Storage Parameters for tables (SE13);
- Database Utility (SE14);
- Data Dictionary Information System (SE15);
- Program Maintenance (SE38); and
- Screen Painter (SE51)

We identified 45 users with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object

The maintenance of source code in production should be highly restricted to a Super User Emergency ID following specific procedures with compensating controls. Finally, no one should have access to change dynpros in production.

Recommendation 9

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_DEVELOP for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. The ITS branch will initiate this recommendation in Q2 2007.

Transport Management (S_TRANSPRT)

The SAP authorization object (S_TRANSPRT) allows for the creation of corrections to transport requests as well as the movement of system objects between SAP instances. It also allows access to the Workbench Organizer.

Some of the transactions, which require this object, include:

- Transport System (SE01);
- Install Workbench Organizer (SE06);
- Customizing Request Management (SE10); and
- Documentation (SE61).

We identified 10 users with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object.

Importing and exporting changes or data between systems provides a high degree of risk for overwriting objects across SAP R/3 instances and clients impacting data integrity and system processes. It is critical to understand a transport cannot be "undone", so it is very important to ensure the CTS process is tightly controlled.

This is the authorization for creating development projects and objects and, consequently, it should usually be restricted to configurators and/or BASIS support. If access is needed in production, a process of authorization, review, and approval should be in place.

Recommendation 10

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_TRANSPRT for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

The ITS branch will initiate this recommendation in Q2 2007.

Administration of the Change and Transport System (S_CTS_ADMI)

The SAP authorization object S_CTS_ADMI controls the administration of the Change and Transport System (CTS). The CTS is used to manage changes, modifications, and customizing made to the system and transport them through the pipeline from development to test to production.

We identified nine users with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object. Importing and exporting changes or data between systems raised a high degree of risk for overwriting objects across SAP R/3 instances and clients, thereby impacting data integrity and system processes.

It is critical to understand a transport cannot be "undone", so it is very important to ensure the CTS process is tightly controlled. As a result, if access is required in production, a process of authorization and review should be in place.

Recommendation 11

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_CTS_ADMI for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This action will be initiated in Q2 of 2007.

Changing Client-Independent Tables (S_TABU_CLI)

The SAP authorization object S_TABU_CLI is used in client-independent tables as additional security, and thus complements the general table maintenance authorization. While some staff will need display access, only systems administrators should have access to change these tables. The administrators must understand the possible effects of changes to the tables.

We identified 42 users with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object. Wherever there is more than one client in an instance of SAP R/3 this authorization object carries a risk as it can be used to affect changes in live or protected clients from a test or play client.

This authorization should only be given to well-trained individuals responsible for maintenance who understand the possible effects of changes to tables. In addition, maintenance of tables in production should be restricted to a Super User Emergency ID following specific procedures with compensating controls

Recommendation 12

That Information Technology Services Branch immediately review the users and generic users ids with access to object S_TABU_CLI for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This will be initiated in Q2 of 2007.

Controlling Table Displaying and Maintenance (S_TABU_DIS)

The SAP authorization object S_TABU_DIS is used for controlling table displaying and maintenance through the use of authorization groups, which is fundamental in controlling ongoing use, maintenance, and support of the SAP R/3 system.

SAP R/3 has structured authorization groups by modules (application area), but there are more than 200 tables per module. Further restriction of tables should be required by using authorization groups.

We identified 23 users with varying access to this object, which was greater than was our expectation based on the inherent risk associated with this object.

Access to "01 - create" and "02 - change" should be restricted in the production environment. If create or change is necessary, access should be restricted by authorization group. Consideration should also be given to restricting display access to highly sensitive or confidential information through the use of authorization groups.

Recommendation 13

That Information Technology Services Branch immediately review the users and generic user ids with access to object S_TABU_DIS for reasonableness as well as continue to systematically monitor access levels through their existing authorization audits.

Management Response

Management agrees with this recommendation. This action will be initiated in Q2 of 2007.

5.3 SAP DOCUMENTATION REVIEW

As part of our review of various SAP-based documentation, we reviewed the following for appropriateness and completeness:

- Various SAP IT general control processes;
- The SAP Security Authorizations Strategy;
- The ASAP Business Blueprint; and
- Components of the Integrated Business Systems Project, Stage 1 Strategy report.

We noted numerous instances of documentation that appears to be outdated or in draft format. As a result, there is a risk of inappropriate decision-making based on no longer, fully or partially, applicable documentation. In addition, if used for troubleshooting, maintenance or training purposes, there is an increased likelihood of lost time and effort due to the possible inaccuracy of some of the document contents. Finally, a lack of updated documentation or long-standing draft status may be an indicator of weaknesses in the overall internal control framework, which mandates the requirement for updating and formally approving policies, process descriptions, procedures and key support documents.

More specifically, there are documents dated as far back as 2000, 2002 and 2004. Furthermore, some (the SAP Security Authorizations Strategy) are still noted as being in draft format.

Notwithstanding that, the documentation is easy to follow and user friendly.

Furthermore, we reviewed documentation associated with the initial installation and configuration of SAP that assisted with the automation of certain control activities, or lack thereof. The documentation and the responses therein, demonstrate what was also revealed within the Audit of the Financial Control Environment report. Specifically, there is a significant level of manual controls in place versus having preventive and detective controls with SAP. While the level of automated controls within a business process is highly dependent on the nature in which business is actually conducted, automated preventive controls are more sensitive and timely than manual controls. They support a more robust control environment and, when properly configured, reduce the likelihood of material errors, inappropriate transactions, the need for more time-consuming manual activities, etc.

Recommendation 14

That Information Technology Services Branch require that all relevant SAP-based documentation be:

- **Immediately updated;**

- **Routinely**[18] **updated;**
- **Formally approved and communicated, to represent the current state of each process; and**
- **Incorporated within the scope of their existing document management strategy, which has refresh and update requirements.**

Management Response

Management agrees with this recommendation.

The ITS Branch recognizes the importance and necessity of maintaining current documentation. Workload demands, staff vacancies, and the volume of documentation dictate that different priorities are placed on different document types. System administration procedures and system configuration are given the highest priorities. The Branch will formally implement a document process for high priority documents to ensure they are approved, periodically reviewed and updated.

The ITS Branch identifies a requirement for a technical document writer to assist with document preparation and updating (140 days @ $600 per day – $84,000) to be initiated in Q3 2007 depending on resource availability.
In the case of business process documents, the ITS Branch relies on business process owners to vet all requested SAP change requests to ensure they comply with acceptable business practices and procedures. In the case of major changes or addition of controls, business acceptance testing is also performed.

6 CONCLUSION

Controlling access to its information technology system(s) is a key component for any corporation to uphold a robust control environment. Successful internal controls must therefore start with management stringent access restriction and continuous review of its access administration framework for non-compliance and excessive access. In our opinion, the City may have a greater number of privilege users, than typically expected, posing a potential risk to the City's Corporate Financial Management System (SAP).

The existing IT general controls were found to be well designed. However, we found a lack of consistent internal control activities associated with the logical access and program change management process.

[18] Generally accepted guidelines on regularity include a minimum of once a year assessment, or in conjunction with material environmental changes, for continued applicability. Furthermore, as part of any significant SAP project activity, there should be a required procedures/step to "Assess the impact of the project to existing documentation and updating thereof".

Clear and readily accessible documentation is indicative of sound internal controls. Although SAP-based documentation was available for review, these were found to be in long-standing draft form and therefore may no longer be valid and not reflect the current state of the system. Outdated documentation poses an unnecessary potential risk that changes or steps are no longer relevant or may no longer apply. Improvements are therefore immediately needed to clearly update Corporate Financial Management System (SAP) documentation and a process established to ensure its adequacy and continual review and update.

7 ACKNOWLEDGEMENT

We wish to express our appreciation for the cooperation and assistance afforded the audit team by Management.