SAP Authorizations – Review of Policies, Procedures and Processes©

November 2012

SAP Authorizations – Review of Policies, Procedures and Processes©

November 2012

Table of Contents

Definitions

Due to the technical nature of this report and the need to use terminology unique to SAP and the HRM SAP configuration, the OAG felt the inclusion of a Definitions page would be useful.

BASIS Administrator SAP Administrator	Staff in the Finance and Information, Communications and Technology business unit responsible for the administration and maintenance of the HRM SAP system.
Role	Functionality and permissions for SAP users are through roles. Roles can allow both functionality to transactions, or limit access to, for example, individual cost centres.
Agency Employees	An employee hired through an agency offering temporary workers for short term employment. These hires are not HRM employees but employees of the employment agency.
SAP User Account	A unique user login for the SAP system assigned to an individual.
SAP Employee Record	A record in the SAP Human Resources module for HRM employees. Individual employee records exist for both active and terminated employees.
Active Employee	A current employee of HRM, employed in a position.
Terminated Employee	A former employee of HRM, therefore not currently an active employee. Employment may have ended for a variety of reasons including leaving HRM for other opportunities or retirement for example.
Positions	A job title/classification for individuals employed with HRM. For example HRM has approximately 400 Police Constable positions.
Unique Positions	A job title/classification, where only one individual holds the position or a group of individuals holds the same position. For example, all Police Constables are one unique position as is the single position of CAO held by one person.

Tier 2 Support	Second level of technical support in the Finance and Information, Communications and Technology business unit. The ICT Services Desk (Tier 1) receives calls for service and assigns the request to Tier 2 support for resolution.
SAP Organizational Structure	An intelligent representation (in SAP) of HRM's reporting relationships between positions and individuals. This hierarchy facilitates, for example, electronic authorizations throughout the organization.
Workflow	A sequence of administrative or other processes through which a piece of work passes from initiation to completion.

Executive Summary

The SAP system used by HRM has undergone considerable analysis lately as the Municipality considers its options for the future of the system. This project surrounding SAP authorizations was added to the OAG work plan prior to HRM considering how to best proceed with the provisioning and support of SAP, and it was felt the work should continue regardless of the direction HRM chooses as users, authorizations and roles will continue regardless of future direction.

Throughout the course of this project, we found a recurring theme of undocumented practices rather than written procedures.

Throughout the course of this project, we found a recurring theme of undocumented practices rather than written procedures. Written documentation governing account creation, including who is authorized to request new accounts and changes to existing accounts through to the functionality associated with each SAP role could not be provided to the OAG.

As many as 11% of the accounts were for former employees.

One area where written policy does exist is with respect to employees leaving the organization. However, after the OAG reviewed SAP user accounts on the system in detail, we noted as many as 11% of the accounts was for former employees, which is in violation of the documented procedure.

Most individuals in the same position do not have identical role (SAP permissions) assignments.

Functionality (roles) in SAP is assigned to individual users rather than to positions. Although on the surface the difference appears minor, there is a clear risk of over-assignment of permissions for the requirements of the position (i.e. functionality assigned to an individual but not required as part of their position). Because HRM assigns roles in SAP on the basis of individual users (with no standard template) and not by position, most individuals in the same position do not have identical role (SAP permissions) assignments. The current HRM process raises two concerns: 1) the reasoning for allowing like positions to be set up differently, and 2) the additional effort required to establish individual unique accounts and maintain these accounts.

An over-assignment of functionality may lead to an inappropriate segregation of duties.

The risks of role over-assignment are two-fold. An over-assignment of functionality may lead to an inappropriate segregation of duties where an individual could have enough permissions within the system to complete what would be incompatible tasks, (i.e. an individual requisitioning goods for procurement should not be able

A second risk exists when an individual has access to information not consistent with the duties of the position.

to initiate payment through accounts payable). A second risk exists when an individual has access to information not consistent with the duties of the position.

The recommendations within this report, along with work currently underway by HRM Management in developing written procedures for the creation of SAP authorizations and the creation of an Intake, Transfer and Exit process, will move HRM towards a more secure and standardized use of the SAP system.

Management Response

I have reviewed the Auditor General's report on SAP Authorizations and concur with all of the recommendations. Issues around SAP authorizations have been identified as well, through the SAP due diligence exercise which is nearing completion. As a result, we are about to initiate a project to address authorization issues and will ensure the recommendations of the AG report are specifically addressed through this project.

These process improvements are required regardless of whether SAP support remains here at HRM or migrates to PNS.

- Greg Keefe, Director of Finance & ICT
December 6, 2012

Preamble

The Halifax Regional Municipality utilizes the SAP system as its financial Enterprise Resource Planning (ERP) tool. The initial system installation (version 31H) went live in April 1999, with the Human Resources, Real Estate and Asset Accounting modules being installed after the initial implementation.

The current system configuration utilizes the following SAP modules:

Financials and Controlling (FI CO)
Plant Maintenance (PM)
Material Management (MM)
HR, Payroll & Benefits (HR)
Real Estate (RE)
Asset Accounting (AA)

The last hardware update for the SAP system was completed in November 2004, while the latest installed software update (version) was completed in 2007(Version ECC 6).

Objectives

The overall objective was to determine if appropriate policies, procedures and processes are being used with respect to authorizations and levels of authorizations for use of the HRM SAP system. More specifically:

- to review and gain an understanding of the policies, procedures and processes being used
- to determine if these policies, procedures and processes are both documented and current
- to review and provide comment with respect to controls around activation of accounts, account authorities and changes to authorities upon hiring, position change or leaving the organization
- to review and assess if users authorized to access HRM's SAP system were valid and current employees and were in the same or similar positions for which access was originally granted
- to review and provide comment around controls which oversee authorizations (functional permissions) and to ensure these do not exceed reasonable authorities given the positions of the end users
- to identify other IT systems where similar access controls exist to minimize potential risks to the organization.

Scope

User authorization documentation, SAP user information and employee records were reviewed from April 1, 2010 to present.

Methodology

1. An extraction of SAP users and assigned functionalities was compared with current employees and positions for appropriateness.

2. Validation of authorization requests and approval authority were reviewed for appropriateness.

3. A review of job positions and the roles assigned was done to ensure consistency across positions.

4. Interviews were held with staff of Finance and Information, Communications and Technology.

5. A review of various other related documents.

Summary of Recommendations

2.0.1	The OAG recommends Finance and Information, Communications and Technology create and document a process to capture, log and maintain details of all SAP user account creations and modifications. (Page 14)
2.0.2	For the creation of SAP accounts and assignment of roles (functionality) to accounts, the OAG recommends Finance and Information, Communications and Technology review all policies for effectiveness and controls and commit current practices to written policy/procedures. (Page 14)
2.0.3	The OAG recommends Finance and Information, Communications and Technology ensure the "SAP Employee Change Report Processing Procedure" is followed on termination of employment for the various systems' accesses available to HRM users and further create an internal follow-up procedure to ensure compliance. (Page 18)
2.0.4	The OAG recommends Finance and Information, Communications and Technology examine systems logs for inactive accounts and develop a policy regarding restricting and/or removing access where accounts have not been used for a pre-determined period of time. (Page 18)
2.0.5	The OAG recommends HRM Administration enhance the reliability of the organizational structure within SAP to improve on the success of the ITE process. (Page 19)
3.0.1	The OAG recommends Finance and Information, Communications and Technology migrate towards an authorization model where SAP roles are assigned to positions. (Page 22)
3.0.2	The OAG recommends Finance and Information, Communications and Technology review role assignments to ensure individually assigned accesses do not exceed the needs of the user's employment position. (Page 22)

3.0.3 The OAG recommends Finance and Information, Communications and Technology document the functionality of each role to ensure managers as well as staff responsible for SAP administration of accounts are aware of the total functionality attached to each role assignment. (Page 22)

3.0.4 The OAG recommends Finance and Information, Communications and Technology investigate if any SAP tools are available to assist in highlighting areas where incompatible roles (lack of segregation of duties) might exist. (Page 23)

4.0.1 The OAG recommends Finance and Information, Communications and Technology develop an acceptable use policy for access to and use of HRM systems. Along with the policy, HRM should develop a process to inform all users of the need for the highest levels of confidentiality and protection of all HRM data. (Page 25)

4.0.2 The OAG recommends Finance and Information, Communications and Technology implement restrictions within the role definitions to allow access to only that financial information necessary for the position or for the assigned areas of responsibility. (Page 25)

Detailed Findings and Recommendations

1.0 HRM SAP System

The Halifax Regional Municipality utilizes an SAP system as the financial Enterprise Resource Planning (ERP) tool. Quite simply, an ERP tool is defined as an integrated information system which serves all departments within an enterprise. Evolving out of the manufacturing industry, ERP implies the use of packaged software rather than proprietary software written by or for one organization. Requiring varying degrees of effort, ERP modules may be able to interface with an organization's other software and, depending on the software, ERP modules may be alterable using the vendor's proprietary tools as well as proprietary or standard programming languages.[1]

HRM adopted the current system, with SAP Version 31H in April 1999. The initial implementation offered the following modules:

(FI CO) Financials and Controlling
(PM) Plant Maintenance
(MM) Material Management.

Additional modules were added over time increasing the functionality of the system including:

(HR) HR, Payroll, Benefits
(RE) Real Estate
(AA) Asset Accounting.

The currently installed version of SAP running in HRM is SAP ECC 6.

[1] http://www.pcmag.com/encyclopedia_term/0,2542,t=ERP&i=42727,00.asp

2.0 SAP User Accounts

The Finance and Information, Communications and Technology (FICT) business unit controls user accounts allowing access to the SAP system.

Within the FICT business unit, user account creation, maintenance and removal fall to the Information, Communications and Technology (ICT) division. The SAP/BASIS Administrators are responsible for the creation of user accounts and the assignment of user roles.

Requests for access to the SAP system are initially logged through the ICT Service Desk, and later assigned to SAP/BASIS Administrators. An SAP/BASIS Administrator creates the new account based on the information supplied in the request received by the Service Desk. User accounts are generally created using the first six characters of the last name and first initial of the user. If duplicates exist, an additional initial is added. If the new account request lacks details or appropriate authorization, the SAP Administrator will contact the requestor (usually the direct manager) and seek approvals/clarity before proceeding.

SAP Administrators and Service Desk personnel are working from undocumented practices rather than formal written procedures.

The OAG requested copies of any written procedures currently being used in the creation of user accounts and were told SAP Administrators and Service Desk personnel are working from undocumented practices rather than formal written procedures.

The list of 26 samples provided to ICT for supporting documentation, returned only 9 results where documentation existed.

A random sample of 26 "account creations" was extracted from the 123 accounts created between April 4, 2011 and August 13, 2012[2] to check for proper documentation (i.e. logged and tracked through the Service Desk) and authorizations. The list of 26 samples provided to ICT for supporting documentation, returned only 9 results where documentation existed.

[2] The original request was April 1, 2010 – August 13, 2012 with 240 account creations and a sample size of 49. ICT had done an upgrade April 4, 2011 and records prior to that date were not available. The sampling was subsequently adjusted to reflect the data available.

Table 2.0.1 SAP Account Creation Sample – for appropriate documentation and authorizations

Accounts created after April 4, 2011	**123**
Sample Size	26
Documentation available	9
Authorizations appropriate	9
% of accounts created with appropriate documentation and authorizations	34.6%

The documentation provided by ICT from the Service Desk system showed only 34.6% of the sampled accounts created between April 4, 2011 and August 13, 2012 had an appropriate audit trail available. The documentation which existed supporting the authorizations and/or follow-up appeared reasonable for these nine accounts.

Recommendations

2.0.1 The OAG recommends Finance and Information, Communications and Technology create and document a process to capture, log and maintain details of all SAP user account creations and modifications.

2.0.2 For the creation of SAP accounts and assignment of roles (functionality) to accounts, the OAG recommends Finance and Information, Communications and Technology review all policies for effectiveness and controls and commit current practices to written policy/procedures.

Current SAP User Accounts

27 accounts were identified as outside agency employees, temporary staff, consultants or individuals responsible for the administration HRM's pension plan.

A data extract from the SAP system on August 13, 2012, listed a total of 798[3] separate user accounts in the system. These user accounts were able to be matched to a valid HRM employee with the exception of 27 accounts. These 27 accounts, with the assistance of ICT staff, were identified as outside agency employees, temporary staff, consultants or individuals responsible for the administration HRM's pension plan.

10.9% of all SAP accounts are for individuals who are no longer employed by HRM. The OAG found it interesting and of great concern to discover two individuals' SAP accounts continued to be used after the date they left HRM employment, in one case the last login date was 18 months after the individual left HRM.

The 798 accounts represented 388 unique positions[4] within HRM. The largest single group of employees utilizing SAP are Administrative Assistants at a count of 26 followed by Payroll/Costing Coordinators at 18 individuals. It is interesting to note one of the largest groupings of accounts, with 87 individuals (10.9% of all SAP accounts), are for individuals who are no longer employed by HRM. Additionally, the OAG found it interesting and of great concern to discover two individuals' SAP accounts continued to be used after the date they left HRM employment, in one case the last login date was 18 months after the individual left HRM.

The sharing of account information is almost always a strongly discouraged practice.

HRM has no written policy disallowing the sharing of SAP system logins; however, the HRM e-mail policy does explicitly state the sharing of passwords with other individuals is inappropriate. The sharing of account information is almost always a strongly discouraged practice as organizations lose control of the actual user of the account. This HRM allowed practice is of great concern to the OAG for obvious reasons. In the case of possible abuse, transactions executed from an account where the original "owner" (of the account) is no longer employed, cannot easily be traced to the actual source.

[3] 798 total accounts, 16 accounts are considered system accounts

[4] Unique positions: A job title/classification, where a position is either held by only one individual or a number of individuals hold the same position. For example, all Police Constables are one unique position as is the position of CAO held by one individual.

Employees Leaving HRM – User Accounts

HRM Finance and Information, Communications and Technology have a procedure entitled "SAP Employee Change Report Processing Procedure". This procedure sets out the steps to be followed regarding the removal of systems access[5], for employees leaving HRM. The process document was issued August 15, 2011.

This process is initiated with a nightly, automatically generated report from SAP on all organizational staff changes within HRM (sent to the ICT Service Desk). Staff changes, flagged as terminations are to have access disabled by either Service Desk and/or Tier 2 Support staff. Step 19 of the SAP Employee Change Report Processing reads:

> *Look in the employee's memberships to see if there is membership to other HRM applications requiring a login ID, see HRM System Checklist below. If they have access to Hansen, SAP, etc. send an assignment to the appropriate Tier 2 group to have access disabled to the required system(s). Please be sure to put the following note in the Work Order Description, Original Description:*
> *"Disable [Name of System] access for [Employee Name] as per SAP Employee Change Report for Date (e.g. August 5, 2011)."*
> *Send one assignment with all employees for each separate system, for that particular report date, not individual tickets for each employee.*

55 SAP user accounts remain on the system for employees having left HRM employment, after implementation of the new system.

The OAG data extract of August 13, 2012, was done just prior to the one-year anniversary of this published ICT procedure. Having followed this written procedure should have eliminated, or greatly reduced the number of inactive accounts. Since the establishment of this procedure on August 11, 2011, 55 SAP user accounts remain on the system for employees having left HRM employment after that date. These 55 accounts are included in the 87 noted earlier. This point is raised as there were 33 accounts already on the system at the implementation of the new procedure on August 11, 20111, and we would not have expected to see that number grow.

[5] This procedure sets out the process for restricting Novell, GroupWise, RSA, Hansen, SAP and other systems access on termination of HRM employment.

Inactive SAP User Accounts – Current Employees

From the data extracted on August 13, 2012, the OAG was able to determine the last login (used) date for all accounts. The table below includes accounts of active employees, and excludes the 87 individuals who left HRM employment.

Table 2.0.2 Inactive SAP Accounts 60, 120 and 365 days old and greater

Inactive Period	User Accounts[6] Inactive (cumulative)	User Accounts Inactive (non-cumulative)	% of All Accounts Inactive
>60 days	163	34	20.4
>120 days	129	67	16.2
>365 days	62	62	7.8

The individual reasons for these inactive accounts are beyond the scope of this project; however, inactivity could be an indicator of position change and/or termination not captured through the SAP Employee Change Report Processing Procedure. Any individual accounts not used, or infrequently used, could become a target for possible misuse going undetected by the account owner or HRM.

The SAP Employee Change Report Processing Procedure is not solely for the removal of SAP access as it specifically references other systems and accesses (as listed in Table 2.0.3) to be handled by this procedure.

Table 2.0.3 SAP Employee Change Report Processing Procedure – Systems Checklist

Novell	Blackberry Server	Class
GroupWise	Aventail SSL	Windows Server
RAS	Versadex	Trapeze
Hansen	PDIR	Active Directory
SAP	RAS	Oracle Applications
Hastus	FDM	
Open Text	TrackIT	

[6] Cumulative totals are inclusive of the inactive accounts in the longer periods, i.e. number for >120 days also includes the number for >365.

The OAG, through this project, looked only at SAP access and authorizations, but wonders if similar numbers (for terminated employees and inactive accounts) exist in other systems.

The OAG, through this project, looked only at SAP access and authorizations, but wonders if similar numbers (for terminated employees and inactive accounts) exist in other systems.

Recommendations

2.0.3 The OAG recommends Finance and Information, Communications and Technology ensure the "SAP Employee Change Report Processing Procedure" is followed on termination of employment for the various systems' accesses available to HRM users and further create an internal follow-up procedure to ensure compliance.

2.0.4 The OAG recommends Finance and Information, Communications and Technology examine systems logs for inactive accounts and develop a policy regarding restricting and/or removing access where accounts have not been used for a pre-determined period of time.

Intake, Transfer and Exit Process

In the future, it is also envisioned this system could track assigned items, such as corporate credit cards, keys, cellular devices, equipment and account accesses.

During the course of this review, a newly contemplated process to facilitate the intake of new hires, transfer to new positions and exiting of employees from HRM was explained to the OAG. The Intake, Transfer and Exit (ITE) process will create electronic workflows, setting in motion electronic notifications (e.g. e-mail) and electronic authorizations as employees enter, move or exit the organization. In the future, it is also envisioned this system could track assigned items, such as corporate credit cards, keys, cellular devices, equipment and account accesses, as they are issued to individuals; likewise, the system could alert managers during the exit process of items to be returned or disabled in the case of systems access.

The OAG was advised by staff during interviews, the lack of complete information around the configuration of the organization structure in SAP could impede a full implementation of the ITE process. Currently, the OAG understands a standard SAP organizational structure is applied to all business units or divisions within business units. This structure assumes a pre-determined management structure which may not exist in all situations. The system does not presently accommodate a situation where the management hierarchy does not contain the standard number of levels.

Recommendation

2.0.5 The OAG recommends HRM Administration enhance the reliability of the organizational structure within SAP to improve on the success of the ITE process.

3.0 SAP Role Authorizations

Permissions allowing access to transactions and functionality in SAP are granted through roles. Roles, in the simplest forms, are created to allow access to SAP reports, functions and commands. An example of a role is:

AA:DISPLAY_AA (AA: Display Assest [sic] Accounting)

This role is assigned to the individuals in a group of users within HRM who are tasked with the responsibility of monitoring HRM assets. This SAP role, by its name, suggests those users assigned to it to have Display (or Read Only) access.

Roles may allow total access to functionality in SAP, or roles may only allow limited access by restricting access to, for example, specific cost centres. Access to the HR module is (generally) restricted to specific cost centres allowing managers access to only those employees for which they have some responsibility.

An extract of the roles in SAP as of August 13, 2012 listed 1,074 unique roles.

In summary, within the HRM user base of 798 individual accounts, there are 388 "unique job descriptions – or different jobs" ... for example, there are 18 individuals in the position of Payroll/Costing Coordinator.

The OAG compared employee position data with SAP user data to compare roles assigned to employee positions. In summary, within the HRM user base of 798 individual accounts, there are 388 "unique job descriptions – or different jobs". Of the 388 "different jobs", only 90 have multiple individuals in this job, (for example, there are 18 individuals in the position of Payroll/Costing Coordinator), with essentially 298 people holding their own unique "job" with arguably unique roles assigned to each one individually.

Of the 90 positions where multiple individuals hold the position, only 20% (18 positions) are set up with every individual's role profile identical to all others holding the same employment position. Realizing "like positions" may have separate areas of responsibility (i.e. different Administrative Assistants have access to different cost centres) some variances might be expected, given they work in various business units. However, it remains a manual process creating each individual account uniquely, rather than having each account, within a group of positions (i.e. Payroll/Costing Coordinators), configured identically.

However, an individual from Community and Recreation Services has the same unrestricted access within the HR system.

The OAG did not review all assigned roles for every individual; however, a review of the roles with unrestricted access to all cost centres within the HR module was undertaken. The roles of **HR:CC_ALLCOSTCENTRES** and **HR:CC_READ_ALL** allow unrestricted read access within the Human Resources (HR) module of SAP. As expected, most of the individuals in these roles are from Human Resources or senior Finance staff. The OAG was not expecting to see individuals outside of these groups; however, an individual from Community and Recreation Services has the same unrestricted access within the HR system. Clearly, as noted earlier, the assignment of roles to individuals rather than positions is an area of risk due to the possible over-assignment of permissions for the position or individual in the position. The above finding is an example of this, and why the OAG has concerns.

The OAG has concluded there is a concern with respect to one fundamental internal control, being the strong need to ensure, to the extent possible, there are clearly defined divisions of duties.

The OAG has concluded there is a concern with respect to one fundamental internal control, being the strong need to ensure, to the extent possible, there are clearly defined divisions of duties.

Through interviews with ICT staff, it was determined that policies, procedures and role documentation are not specifically set out in written form and often left, on set up, to the SAP/BASIS Administrator's experience.

Anecdotal evidence provided to the OAG suggests the lack of clearly written policies around account creation and standardization of role assignments may place SAP Administrators in a position of being asked by business unit managers to assign what could be incompatible roles, causing issues with division of duties. With no written documentation on what positions receive what roles and the breadth of each role assignment, the SAP/BASIS Administrators are forced to use judgment and review similar positions to establish permissions for individual users on account creations.

With the lack of documented procedures, incompatible roles could be assigned to a user's account causing concerns with inappropriate segregation of duties or the roles not being within the current position's scope of work.

Similar concerns exist with respect to division of duties as individuals move within the organization.

As individuals move within the organization, their roles in SAP are not automatically altered to reflect a new position.

If roles were assigned to positions, as an individual moved from one position to another, the permissions would remain with the vacated position and would be re-applied once the vacated position was filled.

As individuals move within the organization, their roles in SAP are not automatically altered to reflect a new position. For example, an Accounts Payable Clerk could move to a new position involving, for example, initiating a procurement, and unless the SAP administrators are specifically alerted to this change and a fully functioning system of controls is in place, the individual could retain all the SAP functionality of the Accounts Payable position. This clearly would create an organizational risk. However, if roles were assigned to positions, as an individual moved from one position to another, the permissions would remain with the vacated position and would be re-applied once the vacated position was filled. The employee moving positions would have the applicable permissions assigned appropriate to the new position, having no permissions left from the vacated position. These new permissions would be based upon a standard developed after careful discussion and review for each individual position or job function and would also most importantly be consistent in their application.

Recommendations

3.0.1 The OAG recommends Finance and Information, Communications and Technology migrate towards an authorization model where SAP roles are assigned to positions.

3.0.2 The OAG recommends Finance and Information, Communications and Technology review role assignments to ensure individually assigned accesses do not exceed the needs of the user's employment position.

3.0.3 The OAG recommends Finance and Information, Communications and Technology document the functionality of each role to ensure managers as well as staff responsible for SAP administration of accounts are aware of the total functionality attached to each role assignment.

3.0.4 The OAG recommends Finance and Information, Communications and Technology investigate if any SAP tools are available to assist in highlighting areas where incompatible roles (lack of segregation of duties) might exist.

4.0 Data Confidentiality

Acceptable use policies for individuals do not exist for the various other systems, including SAP.

The Finance and Information, Communications and Technology business unit has developed policies on acceptable use for the e-mail system and access to the internet. Acceptable use policies for individuals do not exist for the various other systems, including SAP. However, Administrative Order 41 - Ethical Conduct Policy, speaks generically to data confidentiality:

> *8) Disclosure of Confidential and Sensitive Information: No Member of Council or employee shall, without proper legal authorization, disclose confidential information concerning the property, government, employees or affairs of the Halifax Regional Municipality; nor shall he/she use such information to advance the financial or personal interest of him/herself or others.*

Although HRM has had limited known data breaches from SAP, they have occurred.

Although HRM has had limited known data breaches from SAP, they have occurred[7]. For example, in April 2010, an e-mail was circulated to HRM councillors and others containing internal budget information from an external "Hotmail" account.

As mentioned in Section 3.0, the possible over-assignment of permissions in SAP for the position or individual in the position is a concern to the OAG. The current configuration of the Finance and Controlling modules does not restrict individuals to cost centre information specific to their areas of responsibility, but rather offers unrestricted access to all cost centres' financial information. It is generally thought, in a properly developed system of internal controls, access to information is restricted to only those needing regular access to the data in order to properly carry out their daily duties. This of course prevents data "surfing or browsing" and possible misuse of the data.

Based on the lack of audit information available for account creation, at least one data breach, data indicating former employees' accounts having been used after their departure, and other situations known to the OAG, the OAG believes there is a general complacency around the sensitivity of information contained within HRM's electronic systems.

[7] April 2010 – Confidential budget and salary information was released publicly.

Recommendations

4.0.1	The OAG recommends Finance and Information, Communications and Technology develop an acceptable use policy for access to and use of HRM systems. Along with the policy, HRM should develop a process to inform all users of the need for the highest levels of confidentiality and protection of all HRM data.
4.0.2	The OAG recommends Finance and Information, Communications and Technology implement restrictions within the role definitions to allow access to only that financial information necessary for the position or for the assigned areas of responsibility.

Appendix A – Management Response

HALIFAX
REGIONAL MUNICIPALITY

PO Box 1749
Halifax, Nova Scotia
B3J 3A5 Canada

December 6, 2012

Larry Munroe, Auditor General
33 Alderney Drive, Suite 620
Dartmouth

Dear Mr. Munroe:

SUBJECT: Auditor General's Report on SAP Authoriztions

I have reviewed the Auditor General's report on SAP Authorizations and concurs with all of the recommendations. Issues around SAP authorizations have been identified as well, through the SAP due diligence exercise which is nearing completion. As a result, we are about to initiate a project to address authorization issues and will ensure the recommendations of the AG report are specifically addressed through this project.

These process improvements are required regardless of whether SAP support remains here at HRM or migrates to PNS.

Yours truly,

Greg Keefe, Director of Finance & ICT

cc: Richard Butts, CAO

Finance & Information, Communications & Technology

Tel: (902) 490- 6308 Fax: (902) 490-8778
E-mail: keefeg@halifax.ca Web Site: www.halifax.ca