Basic Overview

Contents

Programmatic and Structural Controls

There are three areas of risk to always been cognizant of in order to ensure security in any computer system:

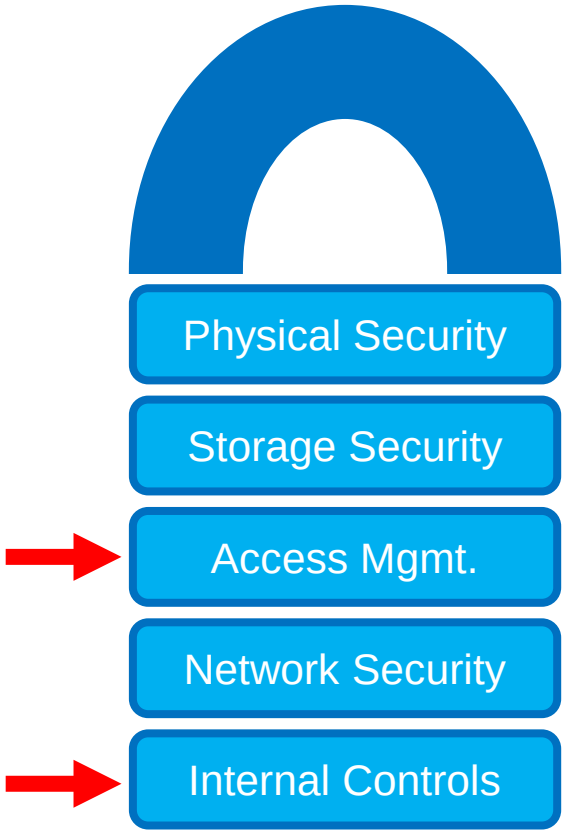
- **Confidentiality:** Unauthorized disclosure of data
- **Integrity:** Unauthorized modification of data
- **Availability:** Denial of service (a lack of availability of computing resources)

The City's SAP deployment is secured using industry-standard systems and best practices. The City has in place security safeguards for the SAP system covering:

- Physical Security (Data Center Access and Physical Systems)
- Network Security (Firewalls, Authentication Systems, VPN Security)
- Malware Prevention (Anti-Virus)
- Security Monitoring (Active Monitoring of the Landscape)
- Incident Management (System Back Up, Disaster Recovery Procedures)
- Etcetera.

There is, of course, are additional layers of security in SAP and that is the focus of this document: To explain to you, the end-user of the system, the two additional security layers that affect you directly:

- **Role-Based Access Controls in the SAP System**
- **A Policy of Segregation of Duties within the Roles**



Role-Based Security

In the SAP system, both application security and unauthorized system access to SAP have to be controlled. The user accounts defined for users in the SAP system are secured by **roles** that grant authorizations to them. SAP authorizations control access to transactions. SAP role authorizations also control what can be performed within a specific business process step by:

- Keeping unauthorized persons out of a specific part of the system
- Safeguarding the data from damage or loss

In SAP, roles are usually related to the job that you do and are closely matched to the business processes mapped to the SAP system.

So a role name may even be the same as the real-world function that an employee performs.

For example:

Timekeepers have the role:
RP_S_TM_TIMEKEEPER

Bureau Buyers have the role:
RP_S_MM_BUREAU_BUYER

Role	From Date	To Date
RP_S_PS_WBS_ELEMENT_COST_PLAN	05/07/2014	12/31/9999
RP_S_HR_BUREAU_SECURITY_REPORT	09/24/2012	12/31/9999
RP_S_OM_HR_BUREAU_SPECIALIST	06/25/2009	12/31/9999
RP_S_OM_BUREAU_OM_REPORTING	06/25/2009	12/31/9999
RP_S_PY_TIMEKPR_PAYROLL_REVIEW	04/12/2012	12/31/9999
RP_C_HR_EMPLOYEE_SELF_SERVICE	09/24/2014	12/31/9999
RP_D_MM_BUREAU_BUYER_PK00	10/18/2016	12/31/9999
RP_S_CO_INTERNAL_ORD_COST_PLAN	05/07/2014	12/31/9999
RP_S_TM_TIMEKEEPER	02/16/2012	12/31/9999
RP_C_LIMITED_PROF_USER_DISPLAY	05/04/2012	12/31/9999
RP_S_PS_BUREAU_CAPITAL_PROJ_AC	05/04/2012	12/31/9999
RP_S_GL_JOURNALS_ENTRIES_PARK	05/04/2012	12/31/9999
RP_S_CO_INTERNAL_ORD_MAINT_STA	05/04/2012	12/31/9999
RP_S_CO_INTERNAL_ORDER_MAINTEN	05/04/2012	12/31/9999
RP_S_FA_BUREAU_ASSET_ACCOUNTAN	05/04/2012	12/31/9999
RP_S_GM_BUREAU_GRANT_ANALYST	05/04/2012	12/31/9999
RP_S_MM_CONTRACT_ADMINISTRATOR	05/04/2012	12/31/9999
RP_S_AR_BILLING_REQUEST_PROCES	05/04/2012	12/31/9999
RP_S_LSO_LEARNER	08/03/2016	12/31/9999
RP_S_CHAG_ROLE_ASSIGN	09/23/2014	12/31/9999

Above: An example set of roles as assigned to an employee. From this you can see that this person is a Timekeeper, Bureau Buyer, General Ledger Processor, and Contract Administrator.

Role-Based Security

What Makes Up A Role?

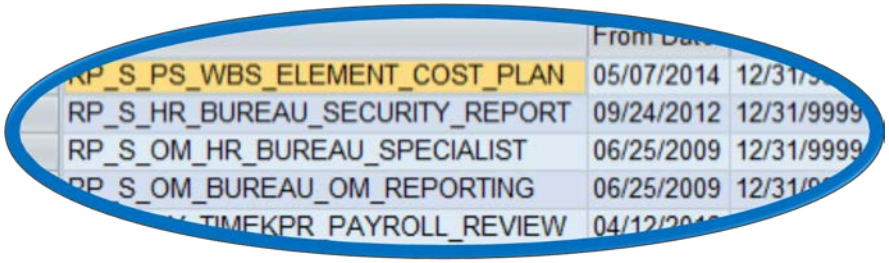
Roles are composed of:

1. **Transaction Codes**
2. **Profile(s)**
3. **Authorization Objects**
4. **Organization Level(s)**

Transaction Codes: SAP Transaction codes transactions are **applications (programs)** that perform a certain function within a given module.

Modules are the functional areas of SAP for specific lines of business like Accounting or Human Resources. Within those larger modules are smaller modules like Accounts Receivable or Payroll.

Specific transactions, like **PA20 – Display HR Master Data** for example, activate a program (the transaction) in the **Personnel Administration module** that permits an authorized user to see personnel data on an employee.



Profile: Profiles are the objects that actually store the authorization data and Roles are the Container that contains the profile authorization data.

Authorization Objects: Objects that define the relation between different fields and also helps in restricting/ allowing the values of that particular field.

Authorization objects are actually defined in programs that are executed for any particular transactions. We can also create custom authorization objects for any particular transaction (generally custom transaction).

Organization Level: This defines actually the organizational elements in SAP. For example, Company Code, Plant, Planning Plant, Purchase Organization, Sales Organization, Work Centers, etc.

Role-Based Security

What Makes Up A Role?

At right is an example of the Timekeeper role expanded to show what transactions (t-codes) are within it.

If you read the t-code title text, you'll see that all the transactions are within the Time Management and Personnel Administration Modules of the larger Human Capital Management (HCM) module. This ensures that a person only granted the Timekeeper role only has access to HR data; not finance or any other kind of data.

However, an individual employee CAN have a Timekeeper role and also be a Financial Analyst giving them access to certain finance data as well. As long as they have authorization to specific roles, there is usually not a problem with someone having roles in multiple modules covering multiple business processes.

There are some exceptions and we'll explain that in the final section covering **Segregation of Duties**.

Transactions in Menu of RP_S_TM_TIMEKEEPER

TCode	Transaction Text...
CADO	Time Sheet: Display Data
CAT2	Time Sheet: Maintain Times
CAT2_ISCR	CATS: Maintain Times (Init. Screen)
CAT3	Time Sheet: Display Times
CATC	Time Sheet: Time Leveling
CATS_DA	Display Working Times
CATSXT_DTL	Work Times: Detail Display
PA20	Display HR Master Data
PA30	Maintain HR Master Data
PA51	Display Time Data
PA61	Maintain Time Data
PO13D	Display Position
PR05	Travel Expense Manager
PT_BAL00	Cumulated Time Evaluation Results
PT_ERL00	Time Evaluation Messages: Analysis
PT_QTA10	Absence Quota Information
PT50	Quota Overview
PT61	Time Statement
PT63	Personal Work Schedule
PT64	Absence List
Y_DRP_630000...	SICK LEAVE W YEARS OF SERVICE
Y_DRP_630000...	TIME SWITCHES IT 2012
ZESS_PAY	Display ESS Pay Statement
ZFI_PYCARE	Payroll Cost Object Validity Report
ZFIPYFOR	Payroll Cost Detail by Employee
ZHR_PYSTOPT...	Pay Statement Print Opted Out List
ZHR_QA_IT2012	BHR QA Check for Pos Pay Std Hrs
ZHR_SICK_HRS	Sick Hours with Years of Service
ZHR_SICKLEA...	Sick Leave Abense Report
ZHR_TIME_SWI...	Time Switches (IT 2012)
ZHR_WORK_O...	Working Out Of Class Report
ZHRT_ABS_QU...	Absence Quota Deductions
ZHRT_CATS_H...	CATS Holiday Audit Report
ZHRT_CUSTOM...	It9005 Custom Audit Report
ZHRT_POLICE_...	Police Over Time Report

Role-Based Security

How Are Roles Assigned?

You receive roles one of two ways:

Automatically

After your Bureau HR processes your new hire or change information you will automatically receive:

New Hires: An SAP User ID and account. This will be communicated to you by your Bureau HR person (usually the Operating Bureau Personnel Administrator (OBPA) or by your Supervisor).

Existing Employees: If you change positions, your new position typically already has the roles you will need on it. You inherit those roles and use your existing SAP credentials to access the system.

Assigned by Manager & Change Agent

If role changes need to be made to your SAP account, usually your supervisor requests that your Bureau Change Agent assign specific roles. Change Agents have knowledge and access to help with such role requests.

If you have a role issue of any kind, let your supervisor know or contact your bureau's Change Agent. A contact list can be found on the EBS website, linked at the right.

Bureau Change Agents (Contact List)

Bureau	Change Agent	Work phone	Alternate | Backup
Auditor's Office	Deborah Scroggin	503-823-3546	Dan Schmidt
BDS	Elshad Hajiyev	503-823-7323	Becky Ault
BES	Lynne Casey	503-823-0593	
BOEC	Genny Dupre	503-823-4655	Victoria Duffey
BPS	Chris Dornan	503-823-6833	
BRFS-Fin Serv	Bill Wagner	503-823-6986	Lois Summers
BRFS-Grants	Black-Craig, Sheila	503-823-6863	
BRFS-PF&T	Andrew Powers	503-823-3101	Michael Montgomery
BRFS-Revenue	Diana Marshall	503-865-2493	Terri Williams
Budget Office	Sarah Diffenderfer	503-823-6925	Jeramy Patton
City Attorney	Kim Sneath	503-823-4047	Crystine Jividen
Council Offices	Ben Smith	503-823-5452	Aaron Beck

LINK: City Change Agents Contact List

Segregation of Duties

Incompatible duties or responsibilities occur when a single person has been given or allowed access that could potentially be used to carry out and conceal errors and/or irregularities in the course of performing their day-to-day activities.

Some examples of incompatible duties are:

- Authorizing a financial transaction, then receiving and maintaining custody of the asset that resulted from the transaction.
- Receiving checks (payment on accounts receivable) and approving write-offs.
- Depositing cash and reconciling bank statements.
- Approving time cards and having custody of paychecks.
- Having unlimited access to alter or adjust assets and accounting records, and computer terminals and programs.

To avoid these kinds of problems certain roles in SAP **CANNOT** be held together by the same employee. The Controller is responsible for ensuring internal controls in all aspects of the City's operations and specific to SAP is in charge of the Segregation of Duties Policy for SAP Role assignments. This policy conforms with the City's law as articulated in administrative rule FIN 6.15 – Internal Controls and Management's Responsibility.

Segregation of Duties is a critical policy to ensure that one employee cannot possess two or more roles in SAP which are a risk to the City's operations.

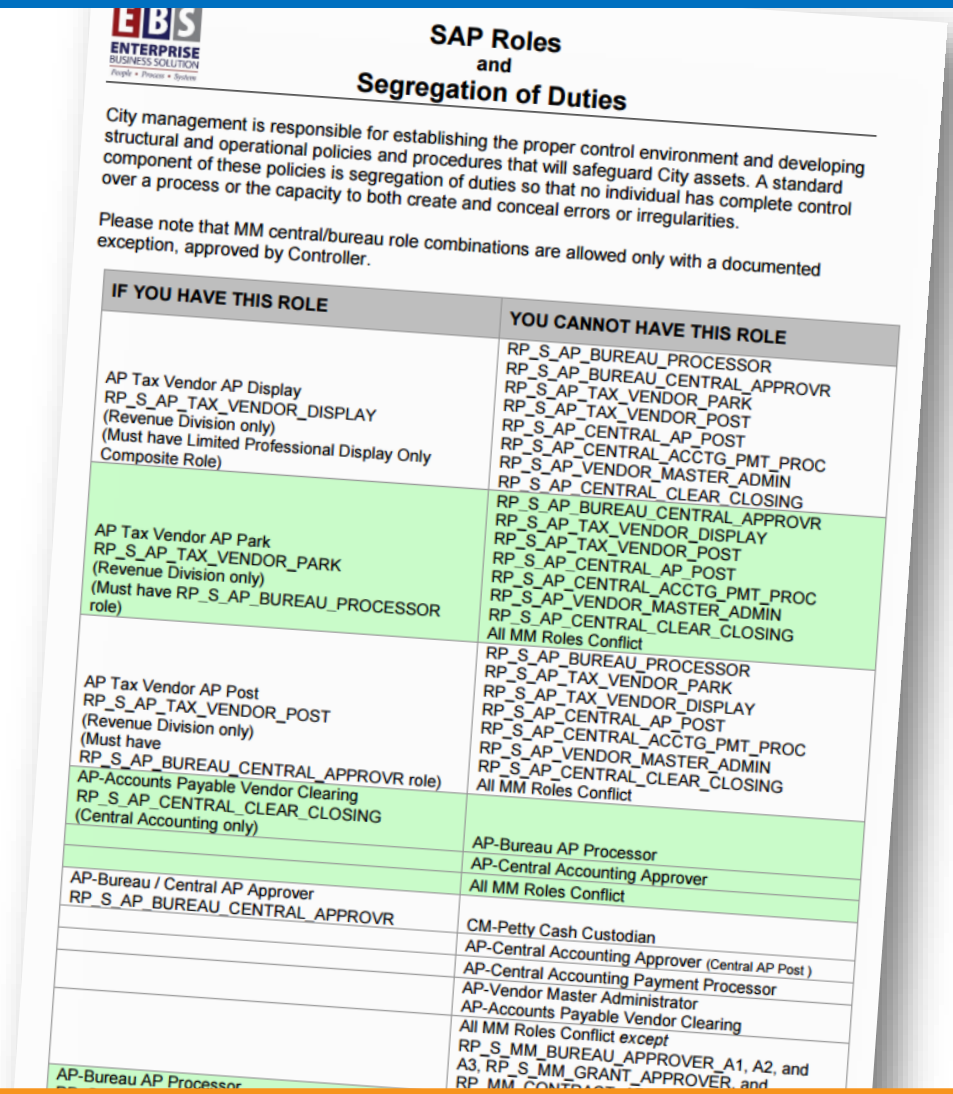
Segregation of Duties

Based on the policy, as set by the controller, the EBS team maps into the role assignment function controls so that conflicting roles are blocked from being assigned to more than one person.

In extremely rare cases, a temporary exception to this process can be granted to the policy. But it must be approved by and monitored by the Controller and the Controller's team. If you require an exception, you must apply through EBS for such an exception. Contact them for more details.

Segregation of Duties List

If you want to know what roles conflict, the EBS Team maintains a current list on their website. It reflects the rules programmed into SAP to ensure conflicting roles are never assigned to the same person. It can be found [HERE].



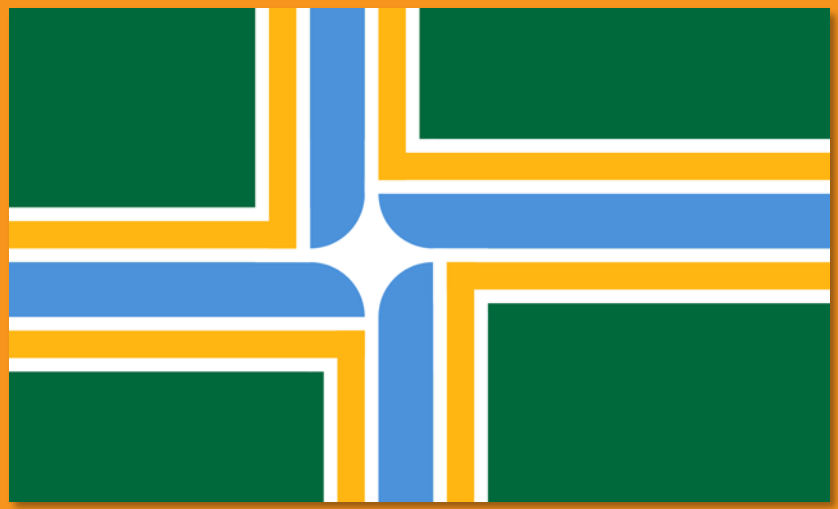
EBS ENTERPRISE BUSINESS SOLUTION

SAP Roles and Segregation of Duties

City management is responsible for establishing the proper control environment and developing structural and operational policies and procedures that will safeguard City assets. A standard component of these policies is segregation of duties so that no individual has complete control over a process or the capacity to both create and conceal errors or irregularities.

Please note that MM central/bureau role combinations are allowed only with a documented exception, approved by Controller.

IF YOU HAVE THIS ROLE	YOU CANNOT HAVE THIS ROLE
AP Tax Vendor AP Display RP_S_AP_TAX_VENDOR_DISPLAY (Revenue Division only) (Must have Limited Professional Display Only Composite Role)	RP_S_AP_BUREAU_PROCESSOR RP_S_AP_BUREAU_CENTRAL_APPROVR RP_S_AP_TAX_VENDOR_PARK RP_S_AP_TAX_VENDOR_POST RP_S_AP_CENTRAL_AP_POST RP_S_AP_CENTRAL_ACCTG_PMT_PROC RP_S_AP_VENDOR_MASTER_ADMIN RP_S_AP_CENTRAL_CLEAR_CLOSING
AP Tax Vendor AP Park RP_S_AP_TAX_VENDOR_PARK (Revenue Division only) (Must have RP_S_AP_BUREAU_PROCESSOR role)	RP_S_AP_BUREAU_CENTRAL_APPROVR RP_S_AP_TAX_VENDOR_DISPLAY RP_S_AP_TAX_VENDOR_POST RP_S_AP_CENTRAL_AP_POST RP_S_AP_CENTRAL_ACCTG_PMT_PROC RP_S_AP_VENDOR_MASTER_ADMIN RP_S_AP_CENTRAL_CLEAR_CLOSING All MM Roles Conflict
AP Tax Vendor AP Post RP_S_AP_TAX_VENDOR_POST (Revenue Division only) (Must have RP_S_AP_BUREAU_CENTRAL_APPROVR role)	RP_S_AP_BUREAU_PROCESSOR RP_S_AP_TAX_VENDOR_PARK RP_S_AP_TAX_VENDOR_DISPLAY RP_S_AP_CENTRAL_AP_POST RP_S_AP_CENTRAL_ACCTG_PMT_PROC RP_S_AP_VENDOR_MASTER_ADMIN RP_S_AP_CENTRAL_CLEAR_CLOSING All MM Roles Conflict
AP-Accounts Payable Vendor Clearing RP_S_AP_CENTRAL_CLEAR_CLOSING (Central Accounting only)	AP-Bureau AP Processor AP-Central Accounting Approver All MM Roles Conflict
AP-Bureau / Central AP Approver RP_S_AP_BUREAU_CENTRAL_APPROVR	CM-Petty Cash Custodian AP-Central Accounting Approver (Central AP Post) AP-Central Accounting Payment Processor AP-Vendor Master Administrator AP-Accounts Payable Vendor Clearing All MM Roles Conflict *except* RP_S_MM_BUREAU_APPROVER_A1, A2, and A3, RP_S_MM_GRANT_APPROVER, and
AP-Bureau AP Processor	



City of Portland

EBS Training & Development

Author: Charlie Dudley, J.D.

2016