MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject:	***Number:***
Role Assignment, Security, and Internal Control Maintenance	205.37 Amended
Date:	***By Direction of:***
March 25, 2013	Kelly Powell Logan, Secretary of Administration Charles B. Zogby, Secretary of the Budget

Contact Agency:
Office of Administration, Office of Human Resources Management, Human Resources Service Center, Telephone 717.787.8001
Office of the Budget, Office of Comptroller Operations, Bureau of Quality Assurance, Telephone 717.425.6830

This directive establishes policy, responsibilities, and procedures for requesting, analyzing, authorizing, establishing, and maintaining the roles necessary for the performance of employee job requirements in the SAP Enterprise Resource Planning system (hereinafter referred to as "SAP"). Marginal dots are excluded due to major changes.

1. **PURPOSE.** To establish policy, responsibilities, and procedures for requesting, analyzing, authorizing, establishing, and maintaining the roles necessary for the performance of employee job requirements in SAP.

2. **SCOPE.** This directive applies to all departments, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction and other agencies using SAP.

3. **OBJECTIVES.**

   a. To preserve the integrity of commonwealth data in SAP and minimize the possibility of errors and misuse of the system for personal gain or harm to the commonwealth.

b. To ensure appropriate system authorization, access to commonwealth data, segregation of duties, and management accountability for role assignments through a uniform process of requesting and assigning roles.

c. To eliminate unnecessary role assignments and limit the number of role assignment changes caused by employee mobility.

d. To assist the Office of Administration, Office for Information Technology (OA/OIT) in ensuring the most economical use of commonwealth SAP software licenses.

4. DEFINITIONS.

a. Business Process Owner (BPO). The person with the authority to determine how a business process should operate and the responsibility to ensure that the process meets ongoing operational needs. Refer to the list of BPOs to identify the person with responsibility and authority for each business process or type of role.

b. Enterprise Personnel Action Request (E-PAR) Form. An electronic form through which supervisors, managers and HR professionals may request services from agency HR offices, document approvals, and facilitate the processing of SAP HR personnel actions. The E-PAR form documents requested changes to employee, position, or organization records, including role requests.

c. Internal Control. A process that provides reasonable assurance that objectives concerning reliability of information, efficient and effective operations, and compliance with applicable laws and regulations are achieved.

d. Master Roles Document. A comprehensive document containing the individual role requirements documents.

e. Mitigating Control. A process that restrains or eliminates risks associated with segregation of duties deficiencies.

f. Role. A collection of tasks performed in SAP necessary to accomplish assigned work. A role may grant access to perform transactions and/or view data. A role may also be defined as the combination of duties, knowledge, and skills an employee uses to fulfill the requirements of a position.

g. Role Conflict. A combination of roles that, due to the transactions assigned to the roles, could allow an error or misuse to occur and remain undetected.

h. Role Requirement Document. A document established for each role that defines: the role; mapping rules; responsibilities; required knowledge, skills, and abilities; necessary tools; and training prerequisites.

i. Rule Set. The governing principles that encompass business processes and functions within the SAP governance, risk management, and compliance (GRC) module and define the SAP transactions that, if assigned to the same user, would result in a segregation of duties risk.

j. SAP Governance, Risk Management and Compliance Module (GRC). The SAP module that houses the business rules and analysis tools used to identify SoD risks. It also serves as a central repository for approved mitigating control information.

k. SAP Software License. The rights to use SAP for commonwealth business that must be procured in advance of accessing SAP functionality.

l. SAP User Account. The SAP master record that identifies the user and contains information such as the employee name, password, and validity dates.

m. Segregation of Duties (SoD). The assignment of roles to different individuals in an effort to eliminate the possibility that a single individual may perpetuate or conceal errors or irregularities.

n. Segregation of Duties (SoD) Waiver. A documented exception that allows a SoD risk to exist for operational reasons based upon the implementation of an approved mitigating control.

o. Simulation Role. The role that allows agency HR offices and HRSC to evaluate SoD risk when assigning roles.

p. Structural Authorization. The organizational authority that is assigned to a role holder for the performance of tasks or access to data inherent to HR and/or payroll roles. Structural authorization determines organizational access or limitations and can be defined at the enterprise, agency, or organization level. Structural authorization applies only to HR and payroll roles.

5. POLICY.

a. All roles must be assigned and maintained by position, not by individual.

b. Agencies must limit role assignments to those necessary to efficiently carry out job functions and business processes.

c. Roles should be assigned to ensure SoD and avoid role conflicts. Roles should not be arbitrarily assigned. If it is determined to be operationally necessary to assign roles in a manner that creates a role conflict, mitigating controls must be documented and approved by the agency head or appropriate designee; reviewed by the Office of the Budget, Office of Comptroller Operations, Bureau of Quality Assurance (BQA); and approved by the appropriate business process owner(s), based on the type of role, through completion of the SoD waiver process.

(1) The Segregation of Duties (SoD) Waiver Request Form must be used by authorized agency HR personnel to request SoD waivers.

(2) Requests for SoD waivers must identify:

(a) The name and position number of the manager accountable for the affected position;

(b) The mitigating control(s) developed to deter and detect errors and inappropriate transactions, as well as the documentation to be maintained relative to the mitigating control(s) and;

(c) Justification for the assignment of conflicting roles.

d. Failure to provide adequate review of business transactions performed by a position with a role conflict assignment may result in disciplinary action, up to and including termination, for the manager accountable for that position.

e. Evidence of the implementation and continuing use of one or more approved mitigating controls must be documented and maintained for the duration of a SoD waiver. Such evidence may be requested during periodic reviews and/or annual audits.

f. SoD waivers approved for an employee's current position will be deactivated when the employee vacates the position; however, a waiver can be reactivated when the position is filled, provided the risk remains and the mitigating control is still in effect.

g. Roles that provide the ability to approve SAP transactions must be assigned only to positions that possess the corresponding organizational authority to approve such transactions.

h. Requests for HR and payroll roles must also include a request for structural authorization that provides adequate organizational access but does not exceed the level of organizational access necessary to perform work-related tasks. Requests for HR and payroll roles with enterprise-wide authorization must be approved by the OA, Deputy Secretary for Human Resources Management.

i. Any misuse of roles and corresponding SAP system access may result in disciplinary action, up to and including termination.

j. Requests to assign roles to contracted personnel must include a description of the nature and duration of the contracted work. Roles may be assigned to contracted personnel only after such a request has been approved by the OA, Deputy Secretary for Human Resources Management (for HR roles) the OB, Deputy Secretary for Comptroller Operations (for finance roles), or the DGS Chief Procurement Officer (for procurement roles).

6. RESPONSIBILITIES.

a. Agency Head or Designee – SoD Waiver Process. Approve or disapprove the use of SoD waivers.

b. Agency HR Offices.

(1) SoD Waiver Process. Complete and submit Segregation of Duties (SoD) Waiver Request Form.

(2) User Provisioning.

(a) Evaluate the SoD risk associated with each E-PAR using the GRC simulation role. If no SoD risk exists, approve the E-PAR and forward it to the HRSC; otherwise, disapprove and close the E-PAR.

(b) Determine if an alternate role or SoD waiver request is appropriate when a SoD risk has been identified. Review organization structures in collaboration with agency managers/supervisors to determine if alternate roles are appropriate.

c. Agency Managers/Supervisors.

(1) SoD Waiver Process.

(a) Identify the need for SoD waivers in collaboration with the agency HR office.

(b) Initiate SoD waiver requests and requests to reactivate waivers, as needed.

(c) Implement mitigating controls associated with approved SoD waivers and maintain operational oversight of fiscal, procurement, HR, and other SAP transactions to prevent fraud, waste, and abuse.

(d) Maintain evidence of the implementation and continuing use of approved mitigating control(s). Allow access to this evidence during periodic reviews or annual audits.

(2) User Provisioning.

(a) Create and submit E-PARs to the respective agency HR office.

(b) Determine if alternate roles are more appropriate when a SoD risk has been identified.

(c) Ensure each employee is trained in the use of the roles that have been assigned to the employee.

d. Office of Administration, Office of Human Resources Management, Human Resources Service Center (HRSC) – User Provisioning.

(1) Evaluate the SoD risk associated with each E-PAR using the GRC simulation role and determine if the E-PAR includes a request for a central role.

(2) Request approval from the appropriate business process owner(s), based on the type of role, for any E-PAR that includes a central role.

(3) Add and/or restrict roles in SAP for each approved role request and process and close the corresponding E-PAR.

(4) Disapprove and close E-PAR requests for central roles when the business process owner(s) have disapproved the assignment of such roles.

e. Business Process Owners (BPO).

(1) SoD Waiver Process. Evaluate SoD waiver requests based on the results of the BQA risk analysis and notify BQA of approvals and disapprovals.

(2) User Provisioning. Evaluate requests for central roles and notify the HRSC of approvals and disapprovals.

(3) Role Management.

(a) Assess each request for a new role to determine if the request includes sufficient justification or an existing role meets the requester's needs.

(b) Submit requests for the creation of new SAP roles or changes to existing SAP roles for analysis and testing in the SAP development environment.

(c) Approve new roles and changes to existing roles based on the results of GRC user and role analyses and successful completion of functionality testing; notify the IES Business Operations Division of such approvals.

(d) Notify the appropriate user group(s) when a new role has been moved to the SAP production environment.

f. IES Business Operations Division – Role Management.

(1) Assist business process owners in determining when new roles are required.

(2) Conduct functionality testing in the SAP development environment for proposed new roles.

(3) Request the movement of approved roles from the SAP development environment to the SAP production environment, upon receipt of business process owner approval.

g. IES Technical Operations Division – Role Management.

(1) Implement changes in the SAP development environment and update the GRC rule set for proposed new roles.

(2) Deactivate proposed role changes that have been disapproved by the business process owners and the portions of the GRC rule set applicable to disapproved role changes.

(3) Move approved roles and role changes from the SAP development environment to the SAP production environment.

(4) Maintain the system relationship between personnel number and position number within SAP.

(5) Evaluate new SAP transaction codes and area menus to determine the roles to which they should be assigned.

h. Office of the Budget, Office of Comptroller Operations, Bureau of Quality Assurance (BQA).

(1) SoD Waiver Process.

(a) Determine if SoD waiver requests are complete; notify the agency of incomplete requests.

(b) Perform GRC risk analysis on SoD waiver requests determined to be complete and provide such analysis to the appropriate business process owner(s), based on the type of role.

(c) Notify agencies of BPO approval or disapproval of SoD waiver requests; provide a copy of each approved SoD waiver request to the requesting agency.

(d) Enter and manage SoD waiver documentation in the SAP GRC module.

(e) Conduct periodic reviews of approved SoD waivers to ensure compliance with this directive.

(2) Role Management. Perform user analysis and role analysis for proposed new roles and changes to existing roles; provide the results of the analyses to the appropriate business process owner(s), based on the type of role.

i. Employees shall use assigned roles only for official commonwealth business.

7. RESOURCES.

a. Integrated Enterprise System Website: www.ies.state.pa.us contains the Master Roles Document and other supplementary information to assist employees, managers, and agency HR offices with role assignment and security.

b. OA, Office of Human Resources Management Website: www.hrm.oa.pa.gov provides quick links to IES forms and resource documents as well as an organizational link to HRSC.

c. Office of the Budget, Office of Comptroller Operations Website: www.budget.pa.gov provides an organization profile for OB, Office of Comptroller Operations and any subordinate organizations and functions.

d. **OA/OIT, Information Technology Bulletin BUS001**, Integrated Enterprise System SAP License Review.

e. **List of Business Process Owners.** This list identifies the people with responsibility and authority for each business process/type of role.

f. **SAP Role Security Procedures Manual.** This manual contains procedures for the development of mitigating controls, agency internal SoD waiver approval, waiver request submission, and waiver approval by BQA and BPOs.

This directive replaces, in its entirety, *Management Directive 205.37,* dated June 13, 2005 and rescinds *Administrative Circular 12-09, Requesting Segregation of Duties Waivers for Role Assignments in the SAP Enterprise Resource Planning System.*