U.S. Department of Justice
Federal Bureau of Prisons

P R O G R A M S T A T E M E N T
OPI: FPI/MIS
NUMBER: 8052.03
DATE: March 19, 2015

Millennium Authorizations

/s/
Approved: Charles E. Samuels, Jr.
Director, Federal Bureau of Prisons

1. PURPOSE AND SCOPE

To establish standards for creating and maintaining access authorizations in the Millennium (otherwise known as SAP) system.

a. Summary of Changes

Directives Rescinded
P8052.02 Millennium Authorizations (9/25/03)

This reissuance incorporates the following modifications:

Multiple changes to the entire document were made to reflect UNICOR's new business practice in SAP Authorizations.

b. **Program Objectives**. The expected results of this program are:

- Roles and responsibilities for the development, maintenance, and assignment of user authorizations in the SAP system will be clearly defined.
- Security of information in the SAP system will be maintained by proper internal controls over user permissions to conduct transactions.

c. **Institution Supplement**. None required. Should local facilities make any changes outside the required changes in the national policy or establish any additional local procedures to implement the national policy, the local Union may invoke to negotiate procedures or appropriate arrangements.

2. RESPONSIBILITIES

This section defines the roles and responsibilities of the following positions within UNICOR:

a**. Role Based Business Process Owners** (role-BPO). The functional personnel responsible for protecting the integrity of the information and processes supported by SAP. BPOs or designees are responsible for:

- Developing and approving written mitigating controls for Segregation of Duty (SOD) risk identified by the GRC tool.
- Approving newly created or changes to existing roles in their functional area.
- Reviewing and approving the re-certification of their functional roles assigned to users.

b. **Senior Executive (Deputy Assistant Director).** The person responsible when a mutual agreement cannot be reached by the granting role-BPO and requestor, the DAD makes the final decision based on all the information given to him/her to grant or deny the request.

c. **SAP Access Administrators (AALC or AALC Service Desk [formerly AALC Helpdesk]).** AALC Service Desk personnel are responsible for monitoring, directing, and developing SAP access. This includes but is not limited to:

- Role creation, maintenance, and deletions based upon role-BPO approval.
- Maintaining license controls for users, and providing ad hoc license reports to all business areas, as well as the final yearly license report to SAP.
- Preparing the annual recertification documents for SAP user accounts.
- Reviewing new SAP user requests and modification to existing accounts, coordinating the approval process of all stakeholders, and issuing direction to the SAP User Administrator in making the actual SAP user account change.

d. **Business Process Analysts Enterprise Resources Planning (ERP).** ERP duties are to help administrators define the technical rules for each business area for approved risk conditions and recommend alternatives to eliminate SOD risks in roles and user assignments.

e. **Internal Control & Compliance Group (ICCG).** ICCG performs risk assessments and mitigating control review on a regular basis to identify new risks, perform periodic testing of rules and mitigating controls, and act as a liaison with external auditors.

f. **GRC Administrator.** The GRC Administrator maintains the Governance, Risk, and Compliance (GRC) Tool. This includes but is not limited to the following functions:

- Maintaining and managing the GRC Compliance Calibrator tool.
- Primary gatekeeper of Segregation of Duties (SOD) compliance and reporting among roles and user accounts
- Maintaining GRC mitigating control (MC) documentation.
- Maintaining GRC reports or monitoring tools to identify SOD conflicts and user access

g. **SAP Security Administrator (ERP).** The SAP Security Administrator maintains security procedures for the SAP environments. This includes but is not limited to:

- Developing SAP security procedures and methods of monitoring.
- Using the GRC Tool to monitor the SAP environment for Segregation of Duties (SOD) compliance and reporting among roles and user accounts.
- Using the GRC Tool to monitor mitigating control (MC).
- Reviewing the role development process and advising about security concerns.

h. **Information System Security Officer (ISSO).** This position is located in MISB and is responsible for security policy compliance throughout FPI. He/she performs audits and generates reports on system security violations to DOJ and FPI management. This position tracks violations and system security changes.

i. **SAP User Administrator.** This position is responsible for creating and maintaining user accounts. He/she is typically the System Administrator, but the duties can be assigned to other positions or automated systems.

j. **License Owners (LO).** Individuals or entities who have authority/own the SAP access licenses for a specific business process or business group; i.e., Branch Chiefs.

k. **Chief Information Officer** (**CIO).** The individual responsible for all information system matters. The CIO is responsible for system administrators. Enterprise Resource Planning is also a section within MISB.

l. **Chief Financial Officer (CFO)**. The individual with ultimate responsibility for financial policy and procedure.

m. **Branch Chief (BC) or General Manager (GM)**. Individual(s) responsible for a business unit within FPI. The Branch Chief/General Manager or designee is responsible for user license approval for new users in his/her unit.

n. **Section Chief Enterprise Resource Planning** (**SCERP).** The individual with ultimate responsibility for all aspects of SAP authorizations. When a decision made for a role or the abuse of role privileges introduces a threat to the security of the SAP environment, the SCERP has the authority to overrule the decision to eliminate or reduce the threat.

3. SAP SYSTEM LOGON ID

Staff, contractors, vendors, and inmates granted access to UNICOR's SAP system are issued only one Logon ID per person.

4. SAP USER ACCOUNT CHANGES

a. **Assignment of SAP Roles.** It is through the approval of the Role-Business Process Owner (role-BPO) that users are approved to use a role to perform a specific task within SAP.

Each SAP user account is validated to ensure that Segregation of Duties (SOD) conflicts are identified and mitigated within SAP, using the (GRC) Tool.

The role is assigned by the SAP User Administrator to the SAP user account. Staff are assigned to approved roles that end with "*staff"* or *"st"* and inmates are assigned to approved roles that end with "*inmates"* or *"in"*.

Functional roles are named and assembled based on specific functions required for a specific job performance. **Example:** The activity group "*Acct*" contains the transactions required to perform an Accountant's duties and responsibilities.

The Temporary Access call type in the helpdesk service ticket system is used when roles assigned either as collateral duty or on a temporary basis result in a segregation of duties (SOD) conflict. The user request is approved or disapproved and the mitigating control approval is completed by the role-BPO.

b. **Users Departing UNICOR.** The SAP User Administrator secures the account when notified that a user is separating or has separated from UNICOR by:

- Removing all roles and profiles from the account.
- Setting the account's user group to "expired."
- Setting the account's "valid through date" to the current system date.
- Setting an administrative lock on the account.

c. **Users Transferring To Another UNICOR Facility.** For users who are transferring to another UNICOR location, the sending SAP User Administrator modifies the account as follows:

- Removing all roles and profiles from the account.
- Setting an administrative lock on the account.

The receiving SAP User Administrator at the new location makes the appropriate assignments based on the new supervisor's request, role-BPO approval, and as directed by AALC.

d. Requesting Changes to Existing Authorizations. When an individual user needs authorization to perform a transaction that his/her assigned role(s) does not permit, he/she should follow the proper chain of command to submit a helpdesk service ticket.

If the authorization cannot be provided through assignment of an existing role, a role modification or new role creation must be initiated. To initiate this change, the pre-existing helpdesk service ticket is approved by the role-BPO. The helpdesk service ticket is closed out and becomes a system change request (SCR) in the Track Record system. The approved changes are completed following the SDLC for ERP Systems Standard Operating Procedure Manual. Changes to user accounts as the result of the SCR process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator helpdesk service ticket.

e. **Annual User Account Recertification.** Recertification requires that every role assigned to a user account is reviewed and approved by the functional role-BPO. Changes to user accounts as a result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator.

f. **Annual Role-BPO Account Recertification.** Recertification requires that every role assigned to a role-BPO account is reviewed and approved by the primary role-BPO or Deputy Assistant Director. Changes to a role-BPO account as a result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator

5. **SEGREGATION OF DUTIES (SOD).**

SODs, formerly referred to as "*Critical combinations,*" are risk(s) or transaction(s) that present an opportunity for an individual to control a process, from beginning to end, without the involvement of others.

The process of segregating is the ability to separate out transactions within a role, or the stacking of roles to eliminate the threat of an individual controlling an entire process, as a matter of security and/or internal control management.

SODs are identified using the GRC Tool that is maintained by the GRC Administrator or designee. A role or SAP user account with roles that present SODs are reported to the role-BPO to either:

- Assign an existing mitigating control.
- Create a new mitigating control.
- Remove the role(s)/transaction(s) causing the conflict from the role or user account.

a. **Mitigating Controls (MC).** This is action taken to monitor activities when a business condition requires personnel to have the opportunity to exploit operational weakness through additional SAP access.

Role-BPOs are responsible for writing MCs to monitor a conflict. The MCs should:

- Identify how specifically the risk is monitored (i.e., t-code).
- Identify how often the risk is monitored.
- Identify who or what tool is responsible for conducting the monitoring task.
- List the potential violations the monitoring task should identify.

The Internal Control & Compliance Group (ICCG) reviews MCs for accuracy and compliance with current policies.

An approved MC is submitted to the GRC Administrator. This position is responsible for:

- Maintaining approved MC documentation.
- Inputting approved MC into the GRC Tool.
- Assigning user(s) to MCs within the GRC Tool.
- Maintaining the role-BPO and monitoring listings within GRC.
- Notifying role-BPOs of any unmitigated SOD conflicts.

■ Generating SOD audits and general reports.

b. **Annual Mitigating Controls Recertification.** Role-BPOs must review the MCs report for all known controlled risks at least annually to maintain compliance with policy and consistency within the SAP environment.

The GRC Administrator executes a SOD User report "*without*" mitigating risk. The role-BPO identifies the MC to apply or which role to remove for each listed user account that has conflicts.

Changes to user accounts as the result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator helpdesk service ticket. Changes to the GRC Tool, as the result of the recertification process, are carried out by SAP Security Administrator.

6. INCIDENT RESPONSE

Violations to the procedures listed in this Program Statement are investigated, and when deemed necessary by FPI's ISSO are reported in accordance with FPI's Incident Response Plan.

REFERENCES

Program Statements
P1237.11 Information Security Programs (10/24/97)

FPI Standard Operating Procedures
System Development Life-Cycle (SDLC) for ERP Systems
SAP Authorization (Production Environment)
SAP GRC Access Control (Production Environment)

ACA Standards
American Correctional Association 2nd Edition Standards for the Administration of Correctional Agencies: 2-CO-1F-06.

Records Retention
For requirements and retention guidance applicable to this program, see the Records and Information Disposition Schedule (RIDS) on Sallyport.