

Agency Security Officer Training

Thursday, May 30, 2019

Content

- Internal Control
- RACF ID
- Passwords
- Agency Security Officers (ASO)
- Security Review
- R*STARS
- Datamart
- OSPS
- ADPICS
- Contacts

Internal Control

A process effected by management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

Internal Control

Oregon's internal control framework is based on the standards set by **The Committee of Sponsoring Organizations of the Treadway Commission (COSO)**.

According to the COSO model, internal control consist of the following five interrelated components:

- *Control environment*
- *Risk assessment*
- *Control activities*
- *Information and communication*
- *Monitoring*



Internal Control

Management of the State is responsible for:

- Establishing and maintaining internal control
- Developing control procedures that ensure the systems access granted to each user is appropriate and consistent with the user's job duties.

As part of the management, Systems Security must perform activities in the form of directive (policies and procedures), preventive (verifying and validating requests), and detective (Semi-annual Security Review) controls in order to achieve effectiveness and efficient resource usage.

OAM 10.10.00 PO

OAM 10.70.00

RACF ID

Resource
Access
Control
Facility ID

- Required for access to financial systems
- Components
 - 3 letters – Agy
 - 2 additional letters
 - 2 numbers AGYXX##
- Temporary Service Workers
 - Job rotations
 - 2nd concurrent agency position
 - Any temporary worker, contractor, student, or volunteer

RACF Requests

- Request is to be from the agency personnel security officer or an HR appointing authority
- Email to:
 - Workday.help@Oregon.gov

Passwords

- No sharing of passwords or User ID's
 - Shared passwords or User ID's will cause revoking from all financial systems
- Resume vs. Reset
 - Resume – knows password but entered incorrectly
 - Reset – password was forgotten or expired
- Who can ask for password?
 - Only the owner of the User ID

Password Resets

Where to send password reset requests

- Mainframe (SFMA and OSPA)
 - DAS.RacfUserAdm@Oregon.gov
 - User includes name, RACF ID, and system name
- Datamart
 - <https://dasapp.state.or.us/DatamartApp>

Agency Security Officers (ASO)

- Establishing ASO – minimum 2 per system
- ASO Responsibilities
- Sending Requests
- Email List for Security Officers

Establishing ASO

- Agency CFO or designate completes and sends Agency Security Officer Notification Form to Systems Security:
 - Designate new security officer.
 - Change authorization rights.
 - Revoke authorization.
- Must be done within one business day of the change event.
- The appointment is effective when the form is received by System Security.

Establishing ASO - continued

The Agency CFO or designate:

- Grants authorization rights for financial systems:
 - R*STARS
 - ADPICS
 - OSPA
 - Datamart
- Assigns semi-annual review responsibilities.

ASO Responsibilities

- Support system security by requesting the lowest level of access that will allow completion of assignments while preserving a reasonable degree of operational efficiency.
- To the best of each security officer's knowledge, provide assurance of no unnecessary access through timely completion of security reviews.

ASO Responsibilities - continued

- Receive information from management.
- Verify current and requested access is compatible and necessary.
- Request inactivation of access no longer needed.
- Communicate with SSO.
- Retain documentation of all requests for 3 years.

Sending Requests

Questions to consider and discuss with the manager requesting access.

- What are the individual's duties?
- Do they have any current access?
- What kind of transactions need to be processed?
- Does the request support sound internal controls?



This form is to be completed and submitted by the designated Agency Security Officer (ASO) for R*Stars, ADPICS, and OSPA.

User Information

User Last Name:	First Name:	RACF ID:	Agency #:	Email: (must be an active address)	Phone:

R*STARS Request

Adjustments to User Class

(use **only** if request varies from the UC template, will apply to all UCs on same line)

Action	User Class(s) Form not valid for UC 78	Acct Trans	Release Flag	Agy Group	Batch Edit Mode	Disburse. Method	Batch Agy	Template adjustment for 96b screen (ex. WRP=0)
▼		▼	▼		▼	▼		
▼		▼	▼		▼	▼		
▼		▼	▼		▼	▼		

Job duties: Required - A short description of activities the requested access will be used for. (Ex. "to review grants and update profiles")

Additional information to support audit trail:

ADPICS Request

Reset an existing User to the following template

Action	User Id Template	Buyer Id	User Level	User Dept	Mailbox Dept	PO Authorization Amt	Bill To
▼		▼					
Dept Authorization				Template adjustments for the 7700 screens			

Job duties: Required - A short description of activities the requested access will be used for. (Ex. "to create and post requisitions")

Additional information to support audit trail:

OSPA Request

To request OSPA access to other agencies, you must be an authorized ASO for that agy. 'DAS only' templates **must** be requested by DAS OSPA Management.

Action	User Type Template	List any additional agency #'s for access
▼		▼

User OR # - Required for OSPA access	Terminal ID	Terminal information is no longer required for OSPA access.
---	-------------	---

Job duties: Required - A short description of activities the requested access will be used for. (Ex. "to enter time and review benefits")

Additional information to support audit trail:

ASO's typed signature:	(signer must send form using 'submit' button, no scans accepted)	Current Date:

Submit by Email

Print Form

Sending Requests - continued

Use this form to make security requests for:

- R*Stars
- ADPICS
- OSPA

(Adobe Reader 8 or higher required to send form)

Sending Requests – continued

Adjustments to User Class

- Only complete this section if the request varies from the User Class template.

R*STARS Request		Adjustments to User Class (use <u>only</u> if request varies from the UC template, will apply to all UCs on same line)						
Action	User Class(s) Form not valid for UC 78	Acct Trans	Release Flag	Agy Group	Batch Edit Mode	Disburse. Method	Batch Agy	Template adjustment for 96b screen (ex. WRP=0)
Add <input type="button" value="v"/>	17, 99	<input type="button" value="v"/>	<input type="button" value="v"/>		<input type="button" value="v"/>	<input type="button" value="v"/>		
Add <input type="button" value="v"/>	48	4 <input type="button" value="v"/>	<input type="button" value="v"/>		<input type="button" value="v"/>	<input type="button" value="v"/>		
<input type="button" value="v"/>		<input type="button" value="v"/>	<input type="button" value="v"/>		<input type="button" value="v"/>	<input type="button" value="v"/>		

Sending Requests – continued

- Job Duties (Required)
 - A brief description of the job duties justifying the specific access requested.
- Examples:
 - Good
 - Review grants and update profiles.
 - Analyze and reconcile revenues.
 - To post purchase orders.
 - Enter time and review benefits.
 - Insufficient
 - Position title.
 - To perform daily duties.
 - New employee.
 - Match XXX's access.
 - Change in RACF.

Job duties: Required - A short description of activities the requested access will be used for. (Ex. "to review grants and update profiles")

Sending Requests - continued

- Requests are sent from authorized ASOs.
- ASOs can not make requests for themselves.
- Datamart requests should be sent separately.
- Access requests are sent to:
Security.Systems@Oregon.gov

Email List for Security Officers

- Subscribe to the ASO News List
- http://listsmart.osl.state.or.us/mailman/listinfo/sfm_a-ospa_agy_security_officers



Semi-annual Security Review

- This is done to comply with the Internal Control guidelines, as well as to monitor and provide reasonable assurance that current user access is appropriate and consistent with the user's job duties.
- Reviews start in February and August of each year.
- Two-part process:
 - SSO verifies ASO assignments with each agency's CFO or designate. SSO provides the ASO contact list for review along with verification forms. CFOs must complete the verification forms by signing, dating, and recording any change and return them to the SSO by the specified due date (only the verification forms).
 - ASO verifies the correctness of the access granted to the agency's users and checks with the users' managers to determine if the level of access is still appropriate. SSO provides system-specific reports for review and analysis along with verification forms. ASOs must complete the verification forms by signing, dating, and recording any change and return them to the SSO by the specified due date (only the verification forms).
- Agencies should retain copies of the ASO contact list and system-specific reports for reference purposes.



Semi-annual Security Review

- System-specific Reports.
 - R*STARS
 - RSTARS 96A. User's security profile (all active users).
 - RSTARS 96B. List of the individual screens the user have authority to view or update (Blank, 0, 1, 2, 3). This report includes only those users of which access differs from the Standard UC Templates.
 - ADPICS
 - ADPICS 7600 & 7650. User's security profile.
 - ADPICS 7700. List of the individual screens the user have authority to view or update (X, I, U, D).
 - ADPICS Approval Path. List of documents, amounts and approval levels by department.
 - OSPA
 - OSPA PUSC. User's security profile and list of the individual screens the user have authority to view or update (N, D, U).
 - NOTE: User Type 78, used to add OSPA Datamart tables.
 - Datamart
 - Datamart Standard View. User's access to SFMA tables, OSPA tables and OSPA groups.

Semi-annual Security Review

- Some recommendations when performing the review:
 - R*STARS
 - Pay special attention to Statewide User classes (01 - 10, 36, 38, 39, 46, 50, 59, 65, 70, 79 – 81) and All Agency View Access (UC78).
 - Check for redundancy (Refer to Redundant User Classes list).
 - Consider the User Class Templates as the “ideal” level of access (R*STARS Security Manual).
 - Since the g6B report shows only those users of which access differs from the Standard UC Templates, all require careful review.
 - OSPA
 - Keep in mind some UT 78 where the DMRT field is “D” will be only for OSPA Datamart tables.
 - ADPICS
 - Since there is a high level of customization, it requires a detailed review.
 - DATAMART
 - Pay special attention to OSPA Agency Groups (“All Agencies & DAS Payroll”).
 - Confirm that the user’s current duties still require Datamart.

A comprehensive and detailed review of all the reports is the only way to ensure that each agency user has the appropriate level of access.

Semi-annual Security Review

PUSC OREGON STATE PAYROLL SYSTEM 05/28/19 PROD

USER SCREEN CONTROL

RACFID: USER78 AGENCY-GP: USRTP NAME: NOT FOUND USER TYPE: 78

EMPLOYEE NUMBER: OR8888888

ADB1 N ADB2 N ADD1 N ADD2 N ADD3 N ADW1 N ADW2 N **DMRT N** D910 N PACH N PAGY N
PCHG N PMNT N PMSG N PPRM N PRPT N PSEC N PSYP N PTB1 N PTB2 N PTD1 N PTD2 N
PTD3 N PTW1 N PTW2 N PTX1 N PTX2 N PUSC N P001 N P002 N P003 N P004 N P005 N
P006 N P007 N P009 N P010 N P020 N P030 N P031 N P032 N P050 N P060 N P070 N
P071 N P090 N P130 N P140 N P160 N P190 N P191 N P192 N P300 N P310 N P320 N
P370 N P420 N P430 N P435 N WARP N WCRP N WRDB N

R*STARS Relational Statewide Accounting & Reporting System

- Security Manual
 - SFMA / OSPA Form guide – pg 2
 - User Class descriptions – pg 3-7
 - Redundant User Classes, Special forms – pg 8
 - Screen 96 A/B & D66 information – pg 9-15

96 A – USER SECURITY PROFILE

- Accounting Trans– page 10 – R*STARS Security Manual
- Release Flag and Disbursement Method – page 11

```
USER ID/CLASS: USER17 17 AGENCY: 107 NAME: FULL EXPENDITURE

ACCOUNTING TRANS: 1          BATCH EDIT MODE: 2
RELEASE FLAG: 0             DISBURSEMENT METHOD: 2
AGENCY GROUP:              WORK HOUR: 0000 2400
AGENCY RANGE 1:           WORK DAY: A
AGENCY RANGE 2:           PRINTER ID:
SECURITY AGENCY: 107      DEFAULT
SECURITY ORG:             ACTION CODE AGENCY:
SECURITY ORG:             ACTION CODE:
PRIOR MO POST IND: Y      VIEW TIN INFO: Y (Y/N)
PRIOR YR POST IND: Y      VIEW BANK INFO: N (Y/N)
FUND OVERRIDE:           STATEWIDE REPORTING: N (Y/N)
```

96 B – USER SECURITY PROFILE

S96B VER 2.0		STATE OF OREGON									
LINK TO:		SECURITY PROFILE									
USER ID/CLASS:		AGY:					NAME:				
D01	D02	D03	D04	D05	D06	D08	D09	D10	D11	D12	
D13	D14	D15	D16	D17	D18	D19	D20	D21	D22	D23	
D24	D25	D26	D27	D28	D30	D31	D32	D33	D34	D35	
D36	D37	D38	D39	D40	D41	<u>D42</u>	D43	D44	D45	D46	
<u>D47</u>	D48	D49	D50	D51	D52	<u>D53</u>	D54	D55	D56	D57	
D59	D61	D62	D63	D64	D66	D67	D71	D73	D80	010	
012	014	017	018	020	021	022	023	024	025	026	
<u>027</u>	28A	28B	<u>029</u>	<u>030</u>	031	033	<u>034</u>	035	036	037	
038	039	041	042	043	43M	044	045	046	047	048	
049	<u>051</u>	<u>052</u>	053	054	055	056	057	058	059	061	
062	063	064	065	066	067	068	069	077	078	079	
080	081	082	084	085	086	087	088	089	090	<u>091</u>	
092	093	094	<u>095</u>	096	097	101	102	103	105	106	
515	518	540	550	<u>WRP</u>	REC	SMR					

EFF START DATE: : EFF END DATE: : LAST PROC DATE:

- Screens accessible to most UC – pg 14

D66 – USER CLASS PROFILE

USER CLASS: 17

TITLE: FULL EXPENDITURE CYCLE

I/E (I=INCLUDE,E=EXCLUDE)

ENTER TRANSACTION CODES SEPARATED WITH EITHER "-" OR ",".

I	167	,	200	-	212	,	217	-	290	,	295	,	402	-
	405	,	409	-	420	,	434	-	435	,	438	-	439	,
	468	-	469	,	599	,	696	-	697					

R*STARS cont.

- UC 78 All Agency View Access Request
 - Online at SARS Security website
<http://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx>
- UC 47 – ASO requests inactive UC
 - BAM analyst requests activation when needed

R*STARS cont.

- Too little or too much access?
 - Too little – won't be able to perform job duties
 - Too much – will have access that's never used

Redundant User Classes:

Some user classes duplicate access (on 96B screen or on D66 T-code access), and would be redundant if a user had others within the same grouping. Below is a list of some of the redundancies. It's possible that a redundant user class might be needed, however an explanation of the need would be required in the access request.

With user class **11** you do not need user classes 24 or 25.

With user class **13** you do not need user classes 24 or 25.

With user class **16** you do not need user classes 24 or 25.

With user class **17** you do not need user class 20 (UC 17, 20, 84, or 88 not allowed w/ UC 28 or 98)

With user class **19** you do not need user classes 11, 16, 24, or 25.

With user class **23** you do not need user classes 24, 25*, or 26.

With user class **25** you do not need user class 24.

With user class **26** you do not need user classes 24 or 25*.

With user class **27** you do not need user classes 11, 13, 16, 19, 23, 24, 25*, 26, 29, 32, 33, 34, or 41.

With user class **29** you do not need user classes 11, 13, 16, 19, 24, 32, 33, or 34.

With user class **31** you do not need user classes 24 or 25*.

With user class **32** you do not need user classes 24 or 25*.

With user class **33** you do not need user classes 24 or 25*.

With user class **34** you do not need user classes 24 or 25*.

With user class **41** you do not need user classes 24.

With user class **98** you do not need user class 28.

Datamart

- Datamart is the platform where all the data from SFMA and OSPA is available for reporting and analysis through the IR Studio query tool.
- Access to SFMA Tables.
 - Requires completion of the Datamart Standard View Access Request Form.
 - Users with this level of access are able to pull information originated in R*STARS and ADPICS at a statewide level.
- Access to OSPA Tables.
 - Requires completion of the Datamart Standard View Access Request Form.
 - Users with this level of access are able to pull information originated in OSPA at a agency or group agency level.
 - To get this level of access, SFMA Tables must also be added.
 - Once the request is completed, users must allow 24 hours to be able to access the OSPA tables (servers require overnight process to update the access).



DAS

DEPARTMENT OF ADMINISTRATIVE SERVICES

CHIEF FINANCIAL OFFICE - SARS

Financial Systems Security
Datamart Standard View Access Request Form
- SFMA and OSPA Tables



The authorized Agency Security Officer (ASO) must complete and submit this form for each user requesting access to the SFMA and OSPA standard Datamart views. For other Datamart access, please contact: PPDB Security at group.PPDB@oregon.gov or PICS Security at ORBITS.Help@oregon.gov for assistance.

SFMA Datamart access is granted with all requests, even if only OSPA Datamart is desired. This form must be submitted electronically by the ASO who signs and dates the request using the 'Submit by E-mail' button provided. No scanned forms are accepted.

All Datamart access is subject to the six-month review process as stated in OAM 10.70.00

User Information
Employee Name: Last, First, MI (as shown in PPDB)
RACF ID:
Employee Number (OR#####)
Email:
Agency Number: (5-digit)
Phone:
Ext.
Agency Name:

Please indicate the standard view(s)
SFMA Tables
Yes Add Access
OSPA Tables
Agency only view
OSPA Agency Group: (Request only if multiple agency views are required and your agency is part of the selected group.)
None
Brief description of job duties requiring access (Ex. To review expenditures for manager's reports)

Access Authorization
ASO's typed signature (signer must send form using the 'submit' button, no scans will be accepted)
Current Date:

Submit by Email Print Form

Datamart

Examples and Exercises

OSPA Security Oregon State Payroll Application

- Requesting User Access
 - Required information on form
 - OSPA User types
 - <https://www.oregon.gov/das/Financial/Payroll/Documents/Introsecurity.pdf>
 - Introduction to OSPA Security document

OSPS User Security Screen

```
RACFID: USER49      AGENCY-GP: USRTP      NAME: NOT FOUND      USER TYPE: 49
EMPLOYEE NUMBER: OR8888888
ADB1 N ADB2 N ADD1 N ADD2 N ADD3 N ADW1 N ADW2 N DMRT N D910 N PACH N PAGY N
PCHG N PMNT N PMSG D PPRM N PRPT N PSEC N PSYP N PTB1 N PTB2 N PTD1 N PTD2 N
PTD3 N PTW1 N PTW2 N PTX1 N PTX2 N PUSC N P001 U P002 D P003 U P004 U P005 U
P006 D P007 D P009 N P010 D P020 U P030 D P031 N P032 D P050 D P060 N P070 D
P071 N P090 N P130 N P140 N P160 D P190 D P191 D P192 D P300 N P310 N P320 N
P370 D P420 N P430 D P435 N WARP N WCRP N WRDB N
```

- Gain access to Report screens only through OSPS.Helpdesk@Oregon.gov
 - WARP
 - WCRP
 - WRDB

OSPS by User Type

- Agency View Only
 - UT 79 - Designed for non-payroll staff - non processing
- Payroll Technician / Manager
 - UT 69 and 68 – For processing payroll
- Timekeeper
 - UT 49 and 48 - Time entry but full system access not required
 - Contact OSPS.Help@Oregon.gov for UT assistance

ADPICS

- Advanced Purchasing & Inventory Control System.
- Security is managed through three different screens:
 - 7600 – Primary User Security (user profile)
 - 7650 – Secondary User Security (interfaces, printing devices, capabilities)
 - 7700 – User Program Security (access control)
- 19 standard user shells. A detailed description of each shell is included in the ADPICS Security Manual (Pages 24-89).
- Approval Paths:
 - 5981 – Document approval path
 - 5982 – Department approval path table
 - 5983 – Commodity approval path table
 - 5985 – Initiating department path table
- Electronic Signatures.
 - 5984 – Signature table maintenance.
 - No form is required.
 - Requests to reset ADPICS signature must be emailed by the ASO (include user's name and RACF ID).

ADPICS

- Buyer ID
 - When request this field, make sure the Buyer ID was previously added by SFMA. Contact your SFMA Analyst about the procedure.
- Example

ADPICS Request							
Reset an existing User to the following template							
Action	User Id Template	Buyer Id	User Level	User Dept	Mailbox Dept	PO Authorization Amt	Bill To
Add ▾	BUYER1 - approv ▾	MED	400	10036	1003699	999,999	04550
Dept Authorization					Template adjustments for the 7700 screens		
100****							
Job duties: Required - A brief description of job duties that require the specific access requested. (Ex. "to create and post requisitions")							
Prepare and post purchase orders							
Additional information to support audit trail:							
* Set printer HIJB - 60 for document POC							

Additional Resources

- Systems Security website
 - <http://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx>
- SFMA Security Manuals
 - ADPICS Security Manual and R*STARS Security Manual are available by request (email to Security.SYSTEMS@oregon.gov to get a copy).
- OSPA Security Manual
 - <http://www.oregon.gov/das/Financial/Payroll/Documents/Introsecurity.pdf>
- Datamart Maintenance Website
 - <https://dasapp.state.or.us/DatamartApp>
- HR Systems & Services website
 - <http://www.oregon.gov/das/HR/pages/index.aspx>

Contacts

- Systems Security
 - Systems Security
 - Security.SYSTEMS@oregon.gov
- OSPS
 - OSPS Help Desk
 - OSPS.HELP@oregon.gov
 - (503) 378-6777
- Datamart
 - Datamart Support
 - Datamart.Support@oregon.gov
- ADPICS
 - Contact your SFMS Analyst
- Mainframe Password Reset
 - DAS RACF Administrator
 - DAS.RACFUserAdm@oregon.gov