



## Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

### **z/OS ROSCOE for RACF Analysis Process and Checklist**

*Modeled After:  
SRR REVIEW PROCEDURES  
z/OS ROSCOE for RACF Checklist  
Developed by DISA for the DOD  
Version 6 Release 7  
January 2015*

# Using Vanguard Security Solutions™ to Complete DISA STIG SRR Review Procedures

DISA Version 6.22

Document Number VSS\_STIG-04222015-135700-622A

April, 2015

## Copyright

© 1989-2010 Vanguard Integrity Professionals-Nevada.

All rights reserved. Printed in the USA.

No part of this publication may be copied, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, for any purpose other than the Licensee's personal use, without express written permission from Vanguard Integrity Professionals-Nevada.

## Trademarks

Vanguard Integrity Professionals, Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, Vanguard Authenticator, Vanguard Cleanup, Vanguard Configuration Manager, Vanguard Enforcer, Vanguard ez/AccessControl, Vanguard ez/SignOn, Vanguard ez/SignOn Deploy, Vanguard ez/Integrator, Vanguard ez/Token, Vanguard GRC, Vanguard IAM, Vanguard Identity Manager, Vanguard Identity & Access Management, Vanguard Governance, Risk Management and Compliance, Vanguard inCompliance, Vanguard Offline, Vanguard OPID Manager, Vanguard PasswordReset, Vanguard Policy Manager, Vanguard Registration Manager, Vanguard SecurityCenter, Vanguard Security Conference, Vanguard Security on Demand, Vanguard Security Solutions, Vanguard Security Suite, AutoPilot, eDistribution, Enterprise-Wise, Vanguard Deploy, Vanguard ez/Security on Demand, Find-it-Fix-it-Fast, Knowledge Expo, Pathway to Profitability, QS/390, QuickGen, Quality Security Framework, Quality Security/390 Suite, Registration Manager, RioVision, RiskMinder, Security on Demand, SmartAssist, SmartLink, SmartPanel, and Vanguard Tokenless Authentication are trademarks or service marks of Vanguard Integrity Professionals-Nevada.

AIX, AS/400, IBM logo and the Business Partner emblem, CICS, DB2, IMS, MVS/ESA, OS/400, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other products mentioned in this publication, including Linux, Red Hat, SUSE, UNIX, Solaris and HP-UX, are trademarks or registered trademarks of their respective owners.

## About This Product

Any software products accompanying this publication are copyrighted and owned by Vanguard Integrity Professionals-Nevada. Use of the software product is governed by the provisions of your License Agreement or the Terms of Use on the envelope in which the software product was sent to you. **Warranty and Limitation of Liability:** VANGUARD warrants that the licensed software products as delivered do not infringe any patent or copyright held by any third party and enforceable under U.S. law. THE FOREGOING WARRANTY IS THE SOLE AND EXCLUSIVE WARRANTY PROVIDED BY VANGUARD UNDER OR IN CONNECTION WITH THE LICENSED SOFTWARE PRODUCTS AND IS IN LIEU OF ALL OTHER WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. UNDER NO CIRCUMSTANCES WILL VANGUARD BE LIABLE TO CUSTOMER FOR ANY OF THE FOLLOWING: (I) ANY DAMAGES CAUSED BY THE FAILURE OF CUSTOMER TO PERFORM ITS RESPONSIBILITIES; (II) ANY THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES; OR (III) ANY LOST PROFITS,

LOSS OF BUSINESS, LOST SAVINGS OR OTHER CONSEQUENTIAL, SPECIAL,  
INCIDENTAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, EVEN IF INFORMED OF  
THEIR POSSIBILITY.

## Table of Contents

___STIG ID: ZROSR000 .....	5
___STIG ID: ZROSR001 .....	6
___STIG ID: ZROSR020 .....	7
___STIG ID: ZROSR030 .....	8
___STIG ID: ZROSR032 .....	9
___STIG ID: ZROSR038 .....	10
___STIG ID: ZROSR040 .....	11

**UNCLASSIFIED**

z/OS ROSCOE for RACF Analysis and Checklist

Version 6 Release 7

\_\_\_**STIG ID: ZROSR000**

**Default Severity:** Category II

- a) Check with your IOA or Systems Programming personnel and compile the list of ROSCOE Installation Datasets, Likely:
1. hlq.ROSCOE.\*\*
  2. From the Administrator Main Menu Choose Option 2 Security Server Commands
  3. then choose Option: 3 Data Set
  4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:  

---
  5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter)and validate that UPDATE or higher access is limited to Systems Programming personnel
  10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and validate that conditional access permits of Update or higher are limited to Systems Programming Personnel as well.
  11. Repeat steps 2 through 10 for all datasets in option a.1
- b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.
- c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

**CCI:** CCI-000213

**CCI:** CCI-002234

**UNCLASSIFIED**

z/OS ROSCOE for RACF Analysis and Checklist

*Version 6 Release 7*

**STIG ID: ZROSR001**

**Default Severity:** Category II

- a) Check with your IOA or Systems Programming personnel and compile the list of ROSCOE STC datasets, Likely:
1. hlq.ROSCOE.sys\*. \*\*
  2. From the Administrator Main Menu Choose Option 2 Security Server Commands
  3. then choose Option: 3 Data Set
  4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:  

---
  5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter)and validate that UPDATE or higher access is limited to Systems Programming personnel
  10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and validate that conditional access permits of Update or higher are limited to Systems Programming Personnel as well.
  11. Repeat steps 2 through 10 for all datasets in option a.1
- b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.
- c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

**CCI:** CCI-001499

**UNCLASSIFIED**  
z/OS ROSCOE for RACF Analysis and Checklist  
*Version 6 Release 7*

**STIG ID: ZROSR020**

**Default Severity:** Category II

- a) Refer to the CA ROSCOE Resources table, in the z/OS STIG Addendum. Ensure that all items in #4 below are true for each resource:
1. From the Administrator Main Menu Choose Option 3 Security Server Commands
  2. then choose Option: 4 General Resource Profile
  3. Next to CLASS type in RO@RES and hit enter
  4. Review each resource in the CA ROSCOE Resources table as follows:
    - a. Verify the resource is defined
    - b. Verify that each UACC is NONE and Warning is set to NO.
    - c. Enter LV or LR next to each resource name.
      - i. Verify that access to each resource is restricted to Appropriate Personnel as defined in the table.
      - ii. Tab down to STANDARD ACCESS section and validate that UPDATE or higher access is limited to Systems Programming personnel.
      - iii. Check the CONDITIONAL ACCESS PERMITS section and validate that conditional access permits of UPDATE or higher are limited to Systems Programming Personnel .
      - iv. Check the Audit section setting and verify that Audit settings are per the CA ROSCOE Resources table.
  5. Repeat steps 4a – 4c for all resources in CA ROSCOE Resources table.
- b) If All items in step 4 are true, there is NO FINDING.
- c) If any item in step 4 is not true, this is a FINDING.

**CCI:** CCI-000035

**CCI:** CCI-002234

## UNCLASSIFIED

z/OS ROSCOE for RACF Analysis and Checklist

Version 6 Release 7

\_\_\_**STIG ID: ZROSR030**

**Default Severity:** Category II

- a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: Do the following for the ROSCOE started task, likely called ROSCOE
  - a. From Analyzer main Menu, go to 3;4; Press <ENTER>
  - b. Key in SORT PROCNAME; Press <ENTER>
  - c. Key in L **ROSCOE**; Press <ENTER>
  - d. If not found then **ROSCOE** is not defined to RACF as a STC user.
  - e. If found but has a R in the M column, review the message and ensure that the following does not appear: VSA346R The user ID does not have the protected attribute. If message exists, then user does not have the PROTECTED attribute. This is a finding.
  - f. If found then you would use the "U" line command to determine if the userid is defined to RACF.
  - g. Key the "U" line command for the **ROSCOE** entry; Press <ENTER>
  - h. The userid is defined to RACF if a userid display appears. If not defined you should see the message "Unable to display".
- b) If the userid for the ROSCOE started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.
- c) If the userid for the ROSCOE started task is not defined to the security database or does not have the PROTECTED attribute, this is a FINDING.

**CCI:** CCI-000764



**UNCLASSIFIED**

z/OS ROSCOE for RACF Analysis and Checklist  
Version 6 Release 7

**STIG ID: ZROSR032**

**Default Severity:** Category II

Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: The name of the roscoe started task is likely ROSCOE.

1. From Analyzer main Menu, go to 3;4; Press <ENTER>
  2. Key in SORT PROCNAME; Press <ENTER>
  3. Key in L ROSCOE; Press <ENTER>
  4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
  5. If not found then ROSCOE is not defined to RACF as a STC user.
- b) If a **STARTED** resource class profile exists for the started task ROSCOE, there is NO FINDING.
- c) If neither a **STARTED** resource class profile or an ICHRIN03 entry exists for the started task for ROSCOE, this is a FINDING.

**CCI:** CCI-000764

**UNCLASSIFIED**  
z/OS ROSCOE for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_\_STIG ID: ZROSR038**

**Default Severity:** Category II

Use Vanguard's Administrator product Validate that CLASS RO@RES is active.

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS option 5 SETROPTS option,
- d) Press <ENTER>
- e) On the SETROPTs screen, locate the CDT Classes prompt, enter 'E' next to it.
- f) Press <ENTER>
- g) Invoke the locate command, Locate RO@RES
- h) Screen print the display showing the attributes of the RO@RES class, including active status
  - 1. If the RO@RES class is ACTIVE there is NOFINDING
  - 2. If the RO@RES class is not ACTIVE there is a FINDING

**CCI:** CCI-000336

**CCI:** CCI-002358

**UNCLASSIFIED**  
z/OS ROSCOE for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_\_STIG ID: ZROSR040**

**Default Severity: Category II**

The following steps are necessary for reviewing the ROSCOE options:

- a) Have the products system programmer display the configuration/parameters control statements used in the current running product to define or enable security. This information is located in the SYSIN DD statement in the JCL of the STC Batch job.
- b) Verify the following specifications:

Keyword	Value
EXTSEC	RACF
ACFEXT	YES
CLLEXT	YES
JOBEXT	YES
LIBEXT	YES
MONEXT	YES
PRVEXT	YES
RPFEXT	YES
UPSEXT	YES

- c) If (b) above is true, there is NO FINDING.
- d) If (b) above is untrue, this is a FINDING

**CCI: - CCI-000035**