



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

### **z/OS CA MIM FOR RACF Analysis Process and Checklist**

*Modeled After:  
SRR REVIEW PROCEDURES  
z/OS CA MIM for RACF Checklist  
Developed by DISA for the DOD  
Version 6 Release 3  
January 2015*

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

DISA Version 6.28

Document Number VTA\_STIG-08012016-105500-628A

August, 2016

## Copyright

© 1989-2013 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 ncompliance, 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: ZMIM0040 .....	4
__STIG ID: ZMIMR000 .....	5
__STIG ID: ZMIMR001 .....	7
__STIG ID: ZMIMR020 .....	9
__STIG ID: ZMIMR030 .....	11
__STIG ID: ZMIMR032 .....	12

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIM0040**

**Default Severity:** Category II

- a) Find the name of the dataset specified in the MIMPARMS DD statement in the CA MIM started task procedure.
- b) Check member MIMINIT in the dataset specified in a) above for the setting of the parameter 'SACFMDAUTH'.
- c) If the setting of this parameter is "ON", there is NO FINDING.
- d) If the setting of this parameter is not "ON", there is a FINDING.

**CCI:** CCI-000035

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIMR000**

**Default Severity: Category II**

- a) Consult with your systems programmer to identify the names of the CA MIM resource sharing product installation datasets (they may likely be called or begin with SYS2.MIMGR, SYS3.MIMGR).
- b) Ensure the following data set controls are in effect for the CA-MIM resource sharing installation data sets:
  - READ access to the CA MIM resource sharing installation data sets is restricted to all authorized users.
  - UPDATE or higher access to the CA MIM resource sharing installation data sets is restricted to systems programming personnel.
  - UACC (None) and NOWARNING are specified for the CA MIM resource sharing installation data sets.
  - The RACF data set rules for the CA MIM resource sharing installation data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) are logged.
- c) Verify as follows:
  - 1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.
  - 2. Tab down to the Data Set rows and type LV next to the dataset profile for the first CA MIM data set.
  - 3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
  - 4. Review the Standard Access List and Conditional Access List on the dataset profile General Information Screen and verify that access is restricted as specified in b) above.
  - 5. Verify the 'Audit Successes' column on the dataset profile General Information screen. Underneath it should be found 'Successes Write' which means that all successful UPDATE access is logged as specified in b) above.
  - 6. Verify the 'Audit Failures' column on the dataset profile General Information screen. Underneath it should be found 'Failures Write' which means that all failed UPDATE access is logged as specified in b. above.
  - 7. Repeat steps 1-6 above for any other CA MIM dataset profiles.
- d) If UPDATE access or higher to the CA MIM installation data sets are restricted to systems programming personnel, there is NO FINDING.
- e) If UPDATE access or higher to the CA MIM installation data sets are not restricted to systems programming personnel there is a FINDING.
- f) If UACC = None and Warning = No there is NO FINDING.
- g) If UACC is not None or Warning is not No, there is a FINDING.

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

- h) If all accesses of UPDATE or higher are logged there is NO FINDING.
- i) If all accesses of UPDATE or higher are not logged, there is a FINDING.

**CCI:** CCI-000213

**CCI:** CCI-002234

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIMR001**

**Default Severity: Category II**

- a) Consult with your systems programmer to identify the names of the CA MIM resource sharing product STC datasets (they may likely be called or begin with SYS3.MIGR).
- b) Ensure the following data set controls are in effect for the CA MIM resource sharing STC data sets:
  - READ access to the CA MIM resource sharing product STC data sets can be given to auditors and authorized users.
  - UPDATE or higher access to the CA MIM resource sharing product STC data sets is restricted to systems programming personnel and/or CA MIM's STCs and/or batch users.
  - UACC (None) and NOWARNING are specified for the CA MIM resource sharing products STC data sets.
  - The RACF data set rules for the CA MIM resource sharing STC data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged if required by the IAO.
- c) Verify as follows:
  1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.
  2. Tab down to Data Set row, type LV next to the dataset profile for the first CA MIM resource sharing STC data sets.
  3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
  4. Review the Standard Access List and Conditional Access List areas on the dataset profile General Information Screen and verify that access is restricted as specified in b) above.
  5. If required by the IAO Verify the 'Audit Successes' and 'Audit Failures' column on the dataset profile General Information screen. They should match the access required (probably 'Successes Write' and 'Failures Write' respectively).
  6. Repeat steps 1-5 above for any other CA MIM resource sharing STC dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the CA MIM resource sharing STC data sets are specified as in b) above, there is NO FINDING.
- e) If UPDATE and ALLOCATE (ALTER) access to the CA MIM resource sharing sets is not restricted as in b. above there is a FINDING.
- f) If UACC = None and Warning = No there is NO FINDING.
- g) If UACC is not None or Warning is not No, this is a FINDING.
- h) If logging is as specified in b. above there is NO FINDING.

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

- i) If logging is not as specified in b) above there is a FINDING.

**CCI:** CCI-001499



**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIMR020**

**Default Severity: Category II**

- a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press ENTER.
- b) Tab down to "Profile". The default CA MIM profile prefix is MIMGR and if the default has been used enter 'MIMGR.\*' as the generic resource profile name and hit enter to bring up the General Resource Profile Summary screen listing all the CA MIM resources.  
To determine if the default profile prefix has been used
  - find the name of the data set specified on the MIMPARMS DD statement of the started task procedure.
  - find member MIMINIT in the dataset
  - the value specified in MIMINIT is the prefix for CA MIM resource profiles.
- c) Check the profiles that are displayed on the General Resource Profile Summary screen. For any profiles on the display that are found in the CA MIM RESOURCE SHARING RESOURCES table found in the z/OS STIG addendum:
  - 1. Verify that they are defined with a UACC=NONE.
  - 2. Type **LR** in the CMD column of each resource name and check that:
    - Warning is set to NO
    - The list of users and conditional access users only include users that belong to the groups specified in the CA MIM RESOURCE SHARING RESOURCES table.

\*\* (To check if a user belongs to one of the groups in the CA MIM RESOURCE SHARING RESOURCES table:

  - Select Option 3;2 from the Administrator Main Menu (Security Server Reports, Group Profiles)
  - On the Group Reports Menu, enter 1 at the Command line (for Group Profile Summary)
  - Then tab down to Group and enter the Group Name from the resources table and hit enter.
  - On the next panel enter '**LV**' next to the group name and hit enter.
  - The 'General Information Screen' that comes up will have the list of Connected Users.
- d) If
  - Warning is not set to NO
  - UACC is not set to NONE
  - or any users are granted access who are not in the CA MIM Resource Sharing Resources table there is a FINDING.
- e) If none of the conditions in d) above are true, then there is NO FINDING.

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**CCI:** CCI-000035

**CCI:** CCI-002234

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIMR030**

**Default Severity: Category II**

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and Tab down to “CLASS: “, type ‘STARTED’ for class name.
- c) Find the CA MIM General Resource profile. If not found go to step k) below.
- d) Find the userid associated with the CA MIM started task under the STDATA segment information of the CA MIM general resource profile.
- e) Go back to Administrator main menu, select 3;1 (Security Server Reports – User Profile) and press ENTER.
- f) Tab down to User ID and enter the User ID found in Step d) above and hit enter.
- g) Page down till the Attributes section of the profile.
- h) Verify that “Protected = Yes”.
- i) If Protected = Yes, there is no FINDING.
- j) If Protected = No, there is a FINDING
- k) If CA MIM is NOT found as a General Resource profile under the STARTED class in c) above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
  - 1. From Analyzer main Menu, go to 3;4 (Online Displays – Started Procedures Analysis) and press ENTER.
  - 2. Look for STARTED in the Source column and CAMIM in the Procname column.
  - 3. If the CA MIM started procedure does not have an R in the “M” column there is NO FINDING (an R in the “M” column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)).
  - 4. If there is an R in the “M” column, there is a FINDING.

**CCI: CCI-000764**

**UNCLASSIFIED**  
z/OS CA MIM for RACF Analysis and Checklist  
*Version 6 Release 3*

**\_\_STIG ID: ZMIMR032**

**Default Severity:** Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter 'STARTED' for class name.
- c) Find the CA MIM started task procname.
- d) If found, there is NO FINDING.
- e) If not found, then check if it is defined in the Started Procedures Table (ICHRIN03) as follows:
  - 1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.
  - 2. Look for STARTED in the Source column and the CA MIM started task proc name in the Procname column
  - 3. If found, there is NO FINDING.
  - 4. If it is not found, there is a FINDING.

**CCI:** CCI-000764