



Using Vanguard Security Solutions to Complete  
DISA STIG SRR Review Procedures

**z/OS BMC MAINVIEW for RACF  
Analysis Process and Checklist**

*Modeled After:  
SRR REVIEW PROCEDURES  
z/OS Mainview 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 ZMVZ\_STIG-04222015-092300-622A

April, 2015

## Copyright

© 1989-2011 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: ZMVZR000 .....	5
___STIG ID: ZMVZR001 .....	6
___STIG ID: ZMVZR020 .....	7
___STIG ID: ZMVZR030 .....	9
___STIG ID: ZMVZR032 .....	10
___STIG ID: ZMVZR038 .....	11
___STIG ID: ZMVZR040 .....	12

**UNCLASSIFIED**

**z/OS BMC MAINVIEW for RACF Analysis and Checklist**

*Version 6 Release 5*

**\_\_\_STIG ID: ZMVZR000**

**Default Severity: Category II**

- a) Check with your IOA or Systems Programming personnel and compile the list of BMC MAINVIEW for z/OS Installation Datasets, Likely:
1. SYS2.BMCVIEW.\*\*  
SYS3.BMCVIEW.\*\*
  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. All Authorized Users (ID(\*) ) are allowed READ (any user may be permitted READ).
  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. All Authorized Users (ID(\*)) are allowed READ.
  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 BMC MAINVIEW for RACF Analysis and Checklist Version 6 Release 5

\_\_\_**STIG ID: ZMVZR001**

**Default Severity:** Category II

- a) Check with your IOA or Systems Programming personnel and compile the list of BMC MAINVIEW STC datasets, Likely:
1. hlq.BMCVIEW.\*\*
  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. 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, BMC Mainview STCs and/or BMC Batch Jobs. READ access can be permitted to Auditors and all authorized users.
  9. 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. READ access can be permitted to Auditors and all authorized users.
  10. Repeat steps 2 through 9 for all datasets in option a.1
- b) If a.7, a.8, and a.9 are all true, there is NO FINDING.
- c) If a.7, a.8, and a.9 are not true, this is a FINDING.

**CCI:** CCI-001499

**UNCLASSIFIED**  
z/OS BMC MAINVIEW for RACF Analysis and Checklist  
*Version 6 Release 5*

\_\_\_**STIG ID: ZMVZR020**

**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 “CLASS “, type #BMCVIEW or whatever class has been set up for BMC Mainview Resources (find out from your IOA) on your system and press ENTER.
  1. Look for the profiles in the “Profile Name” column that are listed in the BMC Mainview resource table, resource column in the z/OS STIG Addendum.
  2. Ensure that they are defined with a UACC=NONE in the UACC column:
  3. If all UACCs are NONE, there is NO FINDING on this point.
  4. If any UACC is not equal to NONE, this is a FINDING.
- c) Type **LR** in the CMD column of each resource name listed in the table below and check that.
  1. Warning = NO.
  2. The access list showing list of users, only includes valid users per the resources table.
  3. The users only have the level of access permitted per the BMC Mainview resource table.

\*\* (To check if a user belongs to one of the groups in the BMC MAINVIEW 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 or
  - any users or groups are granted access who are not in the BMC MAINVIEW Resource Table

**UNCLASSIFIED**

**z/OS BMC MAINVIEW for RACF Analysis and Checklist**  
*Version 6 Release 5*

- or any users or groups are granted access that is not permitted to them per the BMC MAINVIEW resource table there is a FINDING.

e). If none of the conditions in d. above are true then there is NO FINDING.

**CCI:** CCI-000035

**CCI:** CCI-002234



**UNCLASSIFIED**  
z/OS BMC MAINVIEW for RACF Analysis and Checklist  
*Version 6 Release 5*

\_\_\_**STIG ID: ZMVZR030**

**Default Severity:** Category II

- a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: Do the following for the BMC MAINVIEW started task, likely called MV\$CAS or MV\$PAS or MV\$MVS.
  - a. From Analyzer main Menu, go to 3;4; Press <ENTER>
  - b. Key in SORT PROCNAME; Press <ENTER>
  - c. Key in L **MV\$**; Press <ENTER>
  - d. If the STC name is not found then **BMC MAINVIEW** is not defined to RACF as a STC user.
  - e. If STC name is found but has an 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 **BMC MAINVIEW** entry; Press <ENTER>
  - h. The userid is defined to RACF if a userid display appears. If not defined you should see the message "No data to display".
- b) If the userid for the **BMC MAINVIEW** started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.
- c) If the userid for the **BMC MAINVIEW** 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 BMC MAINVIEW for RACF Analysis and Checklist**  
*Version 6 Release 5*

\_\_\_**STIG ID: ZMVZR032**

**Default Severity:** Category II

- a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: The name of the BMC Mainview started task is likely MV\$CAS and/or MV\$PAS and/or MV\$MVS
  - 1. From Analyzer main Menu, go to 3;4; Press <ENTER>
  - 2. Key in SORT PROCNAME; Press <ENTER>
  - 3. Key in L MV\$; Press <ENTER>
  - 4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
  - 5. If not found then BMC Mainview is not defined to RACF as a STC user.
- b) If a **STARTED** resource class profile exists for the BMC Mainview started task, there is NO FINDING.
- c) If neither a **STARTED** resource class profile or an ICHRIN03 entry exists for the for BMC Mainview started task, this is a FINDING.

**CCI:** CCI-000764

**UNCLASSIFIED**  
z/OS BMC MAINVIEW for RACF Analysis and Checklist  
*Version 6 Release 5*

**STIG ID: ZMVZR038**

**Default Severity: Category II**

- a) Determine which class is being used for BMC MAINVIEW for z/OS, RACF Security.
- b) Use Vanguard's Administrator product validate that the CLASS is active.
  - 1. From Administrator main menu, select option 2. Security Server Commands.
  - 2. Select SETROPTS option 5 SETROPTS option,
  - 3. On the SETROPTS screen, locate the CDT Classes prompt, enter 'E' next to it.
  - 4. Invoke the locate command, Locate class found in step a.
- c) Screen print the display showing the attributes of the class, including active status
  - 1. If the class is ACTIVE there is NO FINDING
  - 2. If the class is not ACTIVE there is a FINDING

**CCI: CCI-000336**

**CCI: CCI-002358**

**UNCLASSIFIED**  
z/OS BMC MAINVIEW for RACF Analysis and Checklist  
*Version 6 Release 5*

\_\_\_**STIG ID: ZMVZR040**

**Default Severity:** Category II

The following steps are necessary for reviewing the BMC MAINVIEW options:

- a) Have the products system programmer display the configuration/parameters control statements used in the current running product to define or enable security. Refer to the Configuration Location dataset and member specified in the z/OS Dialog Management Procedures for BMC MAINVIEW for z/OS. Verify the following specifications:

Keyword	Value
ESMTYPE	(AUTO RACF)

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

**CCI:** CCI-000035